



Osicom

 **ROUTER***mate*TM

ROUTER *plus* 56K CSU

INSTALLATION AND OPERATION MANUAL

Publication 918-6243 Issue 5, October 1998

Osicom Technologies, Inc.
9020 Junction Drive
Annapolis Junction, Maryland 20701

Phone: 800-359-7710
Local: 301-317-7710
Fax: 301-317-7220
Customer Service: 800-359-2273
Repair: 301-317-7400
World-Wide Web: www.osicom.com
E-mail, product offerings: info@osicom.com
E-mail, technical assistance: support@osicom.com

NOTICE

Osicom Technologies may incorporate enhancements in the product
and change the product specifications described in this manual
at any time and without notice.

Not for use or disclosure to anyone but Osicom Technologies, Inc. customers,
except under written agreement.

© Osicom Technologies, Inc. 1998
Printed in U.S.A.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause such interference, in which case the user will be required to correct the interference at their own expense.

This equipment also meets the technical criteria in the part 68 rules, Subparts A through F (for connection of terminal equipment to the telephone network).

FCC REGISTRATION NUMBER: 1R5USA-24165-DE-N

FCC FACILITY INTERFACE CODE: 04DU5-56, 56,000bps

SERVICE CODE: 9.0F6.0Y

JACK ARRANGEMENTS: Use an RJ48S 8-pin modular telephone jack to connect to the network.

V.32bis modem: Use an RJ11C, 6-pin modular telephone jack to connect to DDD lines.

The wall-mounted transformer (included with the unit) must be used with standalone (desktop) Routermate to assure reliability and compliance to the FCC and Underwriters' Laboratories requirements (as well as Canadian Department of Communications standards, when applicable).

1. INTRODUCTION	1-1
1.1 Overview	1-1
1.2 Features	1-2
1.3 Using this Manual	1-5
2. INSTALLATION	2-1
2.1 Installation Checklist	2-1
2.2 Communications Line Requirements for CSU/DSU	2-2
2.2.1 FCC Part 68 Requirements for CSU/DSU	2-2
2.3 LEDs	2-3
2.4 Interfaces and Cables	2-4
2.5 Management	2-5
2.5.1 Passwords	2-5
2.5.2 Terminal Management	2-5
2.5.3 Telnet/SNMP Management	2-5
2.5.4 Dial-In Management	2-6
2.6 Quick Start Procedure	2-7
2.7 Obtaining the Enterprise MIB	2-9
3. TERMINAL OPERATION	3-1
3.1 Screen Structure	3-1
3.2 Keys and Conventions	3-2
3.3 Terminal Selection	3-3
3.4 Password	3-4
3.5 Main Menu	3-5
3.5.1 Save To Flash	3-5
3.5.2 Logoff	3-5
3.5.3 Screen Path	3-5
4. STATUS AND TEST	4-1
4.1 Screen Structure	4-2
4.2 Status and Test Menu	4-5
4.3 Router Summary	4-6
4.4 CSU Status and Test	4-8
4.4.1 Loopback Tests	4-8
4.4.2 Line Status	4-9
4.5 Interface Status Summary	4-10
4.5.1 LAN Status	4-11
4.5.2 WAN Status (Frame Relay)	4-13
4.5.2.1 Lower Layer Status (WAN)	4-14

4.5.2.2	Annex D Status	4-15
4.5.2.2.1	DLCI Status Table	4-16
4.5.3	WAN Status (PPP)	4-17
4.6	Port Status Summary	4-18
4.6.1	Port Status (LAN - Ethernet)	4-19
4.6.2	Port Status (WAN, Frame Relay)	4-20
4.6.3	Port Status (WAN, PPP)	4-21
4.6.3.1	LCP Status	4-22
4.6.3.1.1	LCP Negotiable Options	4-24
4.6.3.2	IPCP Status	4-25
4.6.3.3	IPXCP Status	4-26
4.6.3.4	BCP Status	4-27
4.7	TCP/IP Status and Test Menu	4-28
4.7.1	Ping/Trace Route	4-28
4.7.2	IP Status	4-30
4.7.2.1	IP Port Counters	4-32
4.7.3	ICMP Status	4-33
4.7.4	TCP and UDP Status	4-34
4.7.4.1	TCP Connection Table	4-36
4.7.5	SNMP Status	4-37
4.7.6	ARP Table	4-39
4.8	IPX Status	4-40
4.8.1	IPX Status (LAN and WAN)	4-41
4.8.1.1	IPX RIP/SAP Status (LAN and WAN)	4-43
4.8.1.2	IPXWAN Status	4-44
4.9	Bridging Status	4-45
4.9.1	Port Bridging Status	4-46
4.10	IP Routing Table	4-47
4.11	IPX Routing Table	4-49
4.12	IPX Services Table	4-51
4.13	Bridging Table	4-52
4.14	Event Log	4-53

5. CONFIGURATION	5-1
5.1 Screen Structure	5-2
5.2 Configuration Menu	5-5
5.3 CSU Configuration	5-6
5.4 Interface Configuration Summary	5-7
5.4.1 LAN Configuration	5-8
5.4.2 WAN Configuration	5-9
5.4.2.1 WAN Protocol Options (Frame Relay)	5-10
5.5 Port Configuration Summary	5-12
5.5.1 Port Configuration	5-13
5.5.1.1 IP Routing Options (LAN)	5-16
5.5.1.2 IP Routing Options (WAN)	5-19
5.5.1.3 IP Filters	5-21
5.5.1.3.1 IP RIP Input/Output Filters	5-23
5.5.1.4 IPX Routing Options	5-24
5.5.1.5 IPX Filters	5-27
5.5.1.5.1 IPX SAP Input/Output Filters	5-29
5.5.1.5.2 IPX RIP Input/Output Filters	5-32
5.5.1.6 Bridging Options	5-34
5.5.1.6.1 Transmit Filters	5-35
5.5.1.7 Encryption Options (Frame Relay and PPP)	5-37
5.6 Global Configuration	5-39
5.6.1 IP Global Configuration	5-40
5.6.1.1 IP Static Routes	5-42
5.6.1.2 IP RIP Neighbor List Table	5-44
5.6.2 IPX Global Configuration	5-45
5.6.3 Bridging Global Configuration	5-46
5.6.3.1 Bridging Static Addresses	5-48
5.6.4 PPP Global Configuration	5-50
5.6.5 Encryption Global Configuration	5-51
6. CONFIGURATION AND SOFTWARE UPDATE (TFTP)	6-1
6.1 Screen Structure	6-1
6.2 Configuration and Software Update	6-2
7. MODEM CONFIGURATION	7-1
7.1 Screen Structure	7-1
7.2 Modem Parameters	7-2

8. UNIT CONFIGURATION 8-1

8.1	Screen Structure	8-1
8.2	Unit Parameters	8-2
8.2.1	System Restart	8-3
8.2.2	System Information	8-6
8.2.3	Service Information	8-7

9. MANAGEMENT CONFIGURATION 9-1

9.1	Screen Structure	9-1
9.2	Management Parameters	9-2
9.2.1	SNMP Trap Client Table	9-2
9.2.2	Traps	9-3

10. MAINTENANCE AND REPAIR 10-1

10.1	Customer Support	10-1
10.2	Equipment Return and Repair	10-1

APPENDIX A. GLOSSARY A-1**APPENDIX B. BASIC NETWORKING PRINCIPLES B-1**

B.1	Local Area Networks	B-2
B.1.1	Ethernet	B-2
B.2	Wide Area Networks	B-3
B.2.1	Point to Point Protocol	B-3
B.2.2	Frame Relay	B-4
B.3	IP Routing	B-6
B.3.1	IP Address	B-6
B.3.2	Subnetworking	B-7
B.3.2.1	Subnet Mask	B-7
B.3.2.2	Class C Subnetworking Using RIP 1	B-8
B.3.2.3	Class C Subnetworking Using Unnumbered WAN Links	B-14
B.3.3	Address Resolution	B-16
B.3.4	RIP	B-18
B.3.5	Types of IP Routes	B-20
B.3.6	IP Filtering	B-22
B.4	IPX Routing	B-23
B.4.1	Frame Types	B-23
B.4.2	Novell Addressing	B-24
B.4.3	Watchdog Spoofing	B-24
B.4.4	RIP	B-26
B.4.5	RIP Filtering	B-28

B.4.6	SAP	B-28
B.4.7	SAP Filtering	B-29

APPENDIX C. INTERFACES AND CABLES C-1

APPENDIX D. ORDERING INFORMATION D-1

APPENDIX E. SPECIFICATIONS E-1

APPENDIX F. MULTIPURPOSE LABEL F-1

APPENDIX G. DIAGNOSTICS G-1

G.1	LED Test	G-2
G.2	RAM Test	G-2
G.3	Flash Test	G-3
G.4	TFTP Software Download	G-4
G.5	System Information	G-5

INDEX

FIGURES

1-1	Routermate Router Plus 56K CSU	1-1
1-2	Router and Bridge Applications	1-1
1-3	Management of the Router	1-2
1-4	System Architecture	1-4
2-1	Rear Panel Connectors	2-4
3-1	Screen Structure	3-1
3-2	Terminal Selection Screen	3-3
3-3	Password Screen	3-4
3-4	Main Menu	3-5
4-1	Screen Structure (Status and Test)	4-2
4-2	Status and Test Menu	4-5
4-3	Router Summary (Frame Relay)	4-6
4-4	Router Summary (PPP)	4-7
4-5	CSU Status and Test	4-8
4-6	Interface Status Summary	4-10
4-7	LAN Status	4-11
4-8	WAN 1 Status (Frame Relay)	4-13
4-9	WAN Lower Layer Status	4-14
4-10	WAN Annex D Status (Frame Relay)	4-15
4-11	DLCI Status Table	4-16
4-12	WAN Status (PPP)	4-17
4-13	Port Status Summary	4-18
4-14	Port Status (LAN)	4-19
4-15	Port Status (Frame Relay)	4-20
4-16	Port Status (PPP)	4-21
4-17	Port LCP Status (PPP)	4-23
4-18	Port LCP Negotiable Options	4-24
4-19	Port IPCP Status (PPP)	4-25
4-20	Port IPXCP Status (PPP)	4-26
4-21	Port BCP Status (PPP)	4-27
4-22	TCP/IP Status	4-28
4-23	Ping/Trace Route Screen	4-29
4-24	IP Status	4-30
4-25	IP Port Counters	4-32
4-26	ICMP Status	4-33
4-27	TCP and UDP Status	4-35
4-28	TCP Connection Table	4-36

Figures

4-29	SNMP Status	4-37
4-30	ARP Table	4-39
4-31	IPX Status	4-40
4-32	Port IPX Status (LAN)	4-41
4-33	Port IPX Status (WAN)	4-42
4-34	Port IPX RIP/SAP Status (LAN and WAN)	4-43
4-35	Port IPXWAN Status (WAN)	4-44
4-36	Bridging Status	4-45
4-37	Port Bridging Status	4-46
4-38	IP Routing Table	4-47
4-39	IPX Routing Table	4-49
4-40	IPX Services Table	4-51
4-41	Bridging Table	4-52
4-42	Event Log	4-53
5-1	Screen Structure (Configuration)	5-2
5-2	Configuration Menu	5-5
5-3	CSU Configuration	5-6
5-4	Interface Configuration Summary	5-7
5-5	LAN Configuration	5-8
5-6	WAN Configuration (Frame Relay)	5-9
5-7	WAN Protocol Options (Frame Relay)	5-11
5-8	Port Configuration Summary	5-12
5-9	Port 0 Configuration (LAN)	5-15
5-10	Port 1 Configuration (WAN; Frame Relay)	5-15
5-11	Port 0 IP Routing Options (LAN)	5-17
5-12	Port 1 IP Routing Options (WAN)	5-19
5-13	IP Filters	5-21
5-14	Port IP RIP Input (Output) Filter Table	5-23
5-15	Port 0 IPX Routing Options (LAN)	5-25
5-16	Port 1 IPX Routing Options (WAN)	5-25
5-17	Port 0 IPX Filters (LAN)	5-27
5-18	Port 1 IPX Filters (WAN)	5-28
5-19	Port 1 IPX SAP Input (Output) Filter Table	5-31
5-20	Port 1 IPX SAP Input (Output) Filter	5-31
5-21	Port 1 IPX RIP Input (Output) Filter Table	5-33
5-22	Port 1 IPX RIP Input (Output) Filter	5-33
5-23	Bridging Options	5-34
5-24	Port Transmit Filter Table	5-36
5-25	Port Transmit Filter	5-36

Figures

5-26	Encryption Options (Frame Relay and PPP)	5-38
5-27	Global Configuration	5-39
5-28	IP Global Configuration	5-40
5-29	IP Static Route Table	5-43
5-30	IP Static Route	5-43
5-31	IP RIP Neighbor List Table (LAN)	5-44
5-32	IPX Global Configuration	5-45
5-33	Bridging Global Configuration	5-47
5-34	Static Address Table	5-48
5-35	Static Address Configuration	5-49
5-36	PPP Global Configuration	5-50
5-37	Encryption Global Configuration	5-51
6-1	Screen Structure (TFTP)	6-1
6-2	Configuration and Software Update	6-1
6-3	Server Address and Filename (w/o SIMM)	6-2
6-4	Initiating File Transfer	6-3
6-5	Configuration File Transfer	6-3
6-6	Software File Transfer	6-4
6-7	Software File Upload	6-4
7-1	Screen Structure (Modem)	7-1
7-2	Modem Menu	7-1
8-1	Screen Structure (Unit)	8-1
8-2	Unit Menu	8-1
8-3	System Restart (Without SIMM)	8-3
8-4	System Restart (With SIMM)	8-4
8-5	System Restart (SW Download in Progress)	8-5
8-6	System Restart (Prompt for Unsaved Configuration Changes)	8-5
8-7	System Information	8-6
8-8	Service Information	8-7
9-1	Screen Structure (Management)	9-1
9-2	Management	9-1
9-3	SNMP Trap Client Table	9-3

Figures

B-1	Local Area Network	B-2
B-2	MAC Addresses on a LAN	B-2
B-3	Wide Area Network	B-3
B-4	Frame Relay Network	B-5
B-5	Point to Point versus Frame Relay Network	B-5
B-6	Class C Subnetworking Example Using RIP 1	B-13
B-7	Class C Subnetworking Example Using Unnumbered WAN Links	B-15
B-8	Packet Delivery Using ARP	B-17
B-9	RIP Advertising Example	B-19
B-10	Direct and Learned Routes	B-20
B-11	Static Route to a Remotely-Booted Device	B-20
B-12	Static Route to a non-RIP Router	B-21
B-13	IPX Frame Types	B-23
B-14	Watchdog Spoofing Disabled	B-25
B-15	Watchdog Spoofing Enabled	B-25
B-16	IPX Transmission Over Fastest Path	B-27
C-1	WAN 1 Cable	C-2
C-2	DDD Line Cable	C-2
F-1	Multipurpose Label - Routermate	F-1
F-2	Multipurpose Label - MiniRack	F-2
G-1	Diagnostic Menu Prompt	G-1
G-2	Diagnostic Menu	G-1
G-3	LED Test	G-2
G-4	RAM Test	G-2
G-5	Flash Test - Flash Info	G-3
G-6	Flash Test - Erase Configuration Flash	G-3
G-7	TFTP Software Download	G-4
G-8	System Information	G-5

TABLES

2-1	LEDs	2-3
3-1	Frequently Used Keys	3-2
5-1	Selected IPX Services	5-30
B-1	Valid Class C Subnetworks	B-9
B-2	Selected IPX Services	B-28
C-1	Console Interface	C-1
C-2	WAN 1 Interface	C-1
C-3	LAN Interface (10BaseT)	C-1
C-4	WAN 2 Interface (V.32 Modem)	C-1
C-5	Router Cables	C-2
D-1	Ordering Information	D-1
E-1	Routermate Plus 56K CSU Specifications	E-1

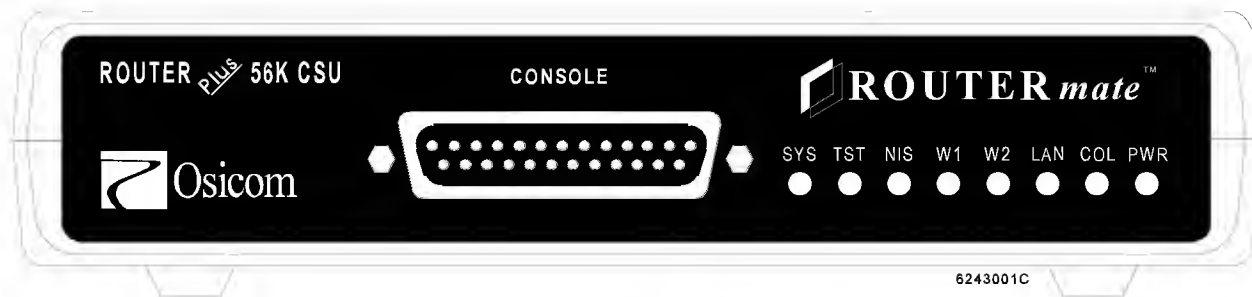


Figure 1-1. Routermate Router Plus 56K CSU

1.1 Overview

Product - ROUTERmate Router Plus 56K CSU

Description - a multi-protocol router and bridge with an integral 56 kbps Channel Service Unit (CSU).

Function - connects 10BaseT Ethernet Local Area Networks (LANs) across AT&T's Digital Data System (DDS) and similar Wide Area Network (WAN) digital services.

Design - the router engine, CSU/DSU, main processor, flash memory, and LAN & WAN interfaces are on the main circuit board. Encryption and V.32 modem options are on separate daughter cards.

1.1	Overview	1-1
1.2	Features	1-2
1.3	Using this Manual	1-4

Definitions

Bridge - Operates at the Data Link Level; it *extends* a network. That is, a bridge connects segments of the same network.

Router - Operates at the Network Level; it *connects* different networks.

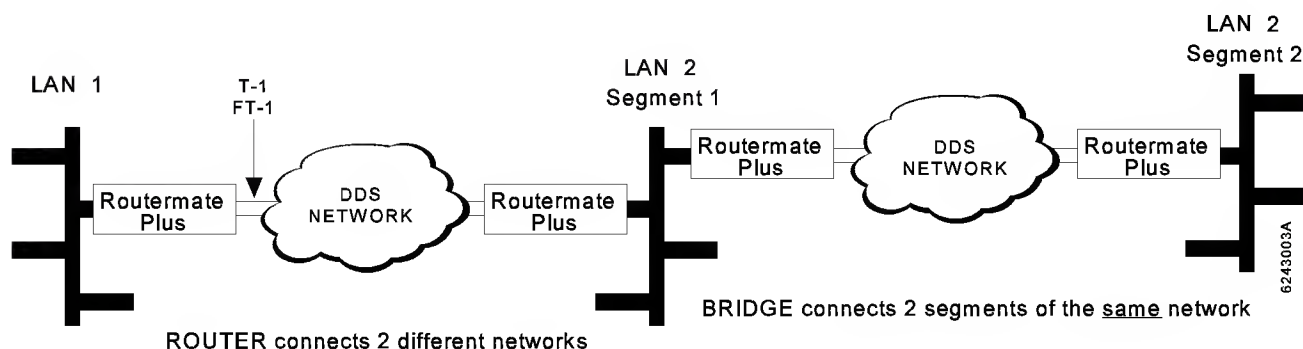


Figure 1-2. Router and Bridge Applications

1.2 Features

Management - (see Figure 1-3)

- VT100 - direct access of the router's management screens through a terminal connected to the front-panel **CONSOLE** interface.
- Telnet - access of the router's management screens from any PC or ASCII terminal on the network using Telnet protocol. The **Telnet Server** parameter on the Management screen defaults to *Enabled*.
- SNMP - access the router's SNMP agent using Simple Network Management Protocol. Refer to Section 2.5.3 for SNMP management capabilities.
- Dial-In Management - an optional internal V.32 modem provides remote dial-up access of the router's management screens over DDS lines. This feature provides a backup management path when the primary path fails. The modem is answer-only.

Integral CSU - internal 56 kbps CSU/DSU (Channel Service Unit/Data Service Unit) provides for direct connection to the 56 kbps DDS service, eliminating the need for a separate CSU and cabling.

Diagnostics - continuously monitors the DDS line and reports any fault so that appropriate action can be taken. A variety of loopbacks and a test pattern generator/comparator are provided. See Section 4.4 for a description of the CSU and DSU telco initiated loopbacks that the Routermate Plus 56K supports.

Front Panel LED Indicators - eight LEDs indicate the operational status of interfaces, tests, and data transmission.

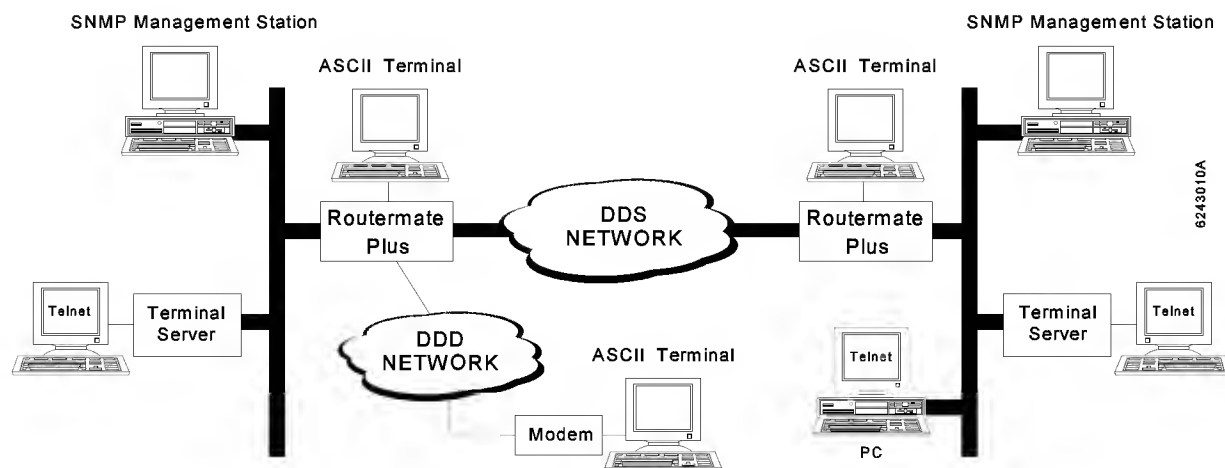


Figure 1-3. Management of the Router

Interfaces -

- 10BaseT (LAN) - 8-pin modular interface connects router to 10Base-T Ethernet Local Area Network.
- WAN 1 - 8-pin modular interface provides the router with a Point-to-Point (PPP) or Frame Relay connection to a 56 kbps Digital Data Service (DDS).
- WAN 2 (optional) - 8-pin modular interface for V.32 modem connects router to dial lines for remote access of the router's management screens. See Modem Configuration in Chapter 7.

Data Encryption - optional encryption hardware provides encryption over PPP and Frame Relay links at speeds up to 1536 kbps.

Encryption is available in standard DES or proprietary E-DES (export) versions.

An additional optional encryption feature lets the user configure the *initial vector*, which is the initial number used to determine how encrypted data is synchronized with the decrypted data, and the *master key*, which is a number that determines the contents of the *encrypted key*. See Appendix D, *Ordering Information*.

The encryption method is based on the Data Encryption Standard (DES) of the National Institute for Standards and Technology.

Bridging - protocols other than IP and IPX can be bridged on both the LAN and WAN interfaces (spanning tree bridging is not supported).

WAN Protocols

- PPP
- Frame Relay
- RFC1490 and Cisco encapsulation
- Inverse ARP

Configuration - configuration is simple because routing is divided into link services (LAN and WAN) and network services (IP, IPX, and bridging). Separate *interface* and *port* configuration screens allow for greater flexibility in configuring links.

Routing Services - the Routermate Plus routes the Internet Protocol (IP) and the Internetwork Packet eXchange (IPX) protocol.

IP includes:

- Transfer Control Protocol (TCP)
- Routing Information Protocol (RIP)
- Address Resolution Protocol (ARP)
- Bootstrap Protocol (BootP)
- Learned or static routes

IPX frames are encapsulated into frame types supported by Novell servers (*Type II*, 802.3, 802.2, and *SNAP*).

IPX includes:

- Service Advertising Protocol (SAP)
- Routing Information Protocol (RIP)
- IPXWAN parameter negotiation

System Architecture - Figure 1-4 illustrates the router's architecture.

- 4 software elements:
 - Network Layer Services
 - LAN Services
 - WAN Services
 - Management
- 1 hardware element: LAN and WAN interfaces.

Management	Network Layer Services IP, IPX Routing and Bridging		
	Port 0	Port 1	Ports 1 - 14
	Ethernet	PPP	Frame Relay
	LAN Interface	WAN Interface	

Figure 1-4. System Architecture

Each service is embedded and knows only the interfaces to service providers (lower layers), service users (higher layers), and management. This design allows flexibility since services at any layer can be enabled, reconfigured, or disabled without affecting the other services.

When using Frame Relay protocol, the router supports up to 15 logical ports (1 for LAN and 14 for WAN 1).

Software and Configuration

- the operating system and parameter configuration are stored on an internal flashROM
- software and configuration uploads and downloads using TFTP
- BootP supported for software downloads

1.3 Using this Manual

Refer to the following for the indicated information:

- Chapter 2, *Installation* - hardware installation and Quick Start procedure.
- Chapter 3, *Terminal Operation* - instructions on how to access and move around in the management screens.
- Chapter 4, *Status and Test* - details of management status screens and CSU testing.
- Chapter 5, *Configuration* - details of configuration parameters.
- Chapter 6, *Configuration and Software Update (TFTP)* - details of downloading and uploading configuration and software files between the router and a TFTP server.
- Chapter 7, *Modem Configuration* - details of configuring the internal modem for dial-in access to the router's management screens.
- Chapter 8, *Unit Configuration* - details of configuring supervisory functions.
- Chapter 9, *Management Configuration* - details of configuring SNMP management parameters.
- Chapter 10, *Maintenance and Repair* - service telephone numbers and instructions for returning faulty equipment.
- Appendix A, *Glossary* - definitions of frequently encountered terms.
- Appendix B, *Basic Networking Principles* - basic routing and bridging concepts and principles.
- Appendix C, *Interfaces and Cables* - interface and cable pin-outs.
- Appendix D, *Ordering Information* - order numbers for all versions of the Routermate Plus 56 CSU and for cables available from Osicom.
- Appendix E, *Specifications* - product specifications and RFC (Request For Comments) compliance.
- Appendix F, *Multipurpose Label* - for convenient reference, a reproduction of the multipurpose label affixed to the bottom of the router.
- Appendix G, *Diagnostics* - details of diagnostic tests and TFTP downloads, which can be performed when powering up the unit.

This chapter provides information on initial installation, configuration, and start-up procedures for your router.

After reading this chapter, you will be familiar with the router's LED indicators and interfaces. Also, you will know how to connect the router to the LAN and WAN and be able to access the router's terminal management screens and configure the router for most applications.

For new installations, see the *Quick Start Procedure* on page 2-7.

Advanced configuration screens are discussed in Chapter 5.

To install rack-mount versions of Routermate products, order the 6-slot MiniRack. Both 115 VAC and -48 VDC power supplies are available. See *Ordering Information* in Appendix D.

2.1	Installation Checklist	2-1
2.2	Communications Line Requirements for CSU/DSU	2-2
2.2.1	FCC Part 68 Requirements for CSU/DSU	2-2
2.3	LEDs	2-3
2.4	Interfaces and Cables	2-4
2.5	Management	2-5
2.5.1	Passwords	2-5
2.5.2	Terminal Management	2-5
2.5.3	Telnet/SNMP Management	2-5
2.5.4	Dial-In Management	2-6
2.6	Quick Start Procedure	2-7
2.7	Obtaining the Enterprise MIB	2-9

2.1 Installation Checklist

Before you begin installation:

1. Upon arrival of the equipment, inspect the condition of the received cartons and compare all items to the packing list attached to the carton.

Appendix D, *Ordering Information*, specifies items included with each sales feature.

NOTES

Notify both Osicom Technologies' Customer Service Department (1-800-359-2273) and the transportation carrier *immediately* if there are any damages or shortages.

Save the cartons and foam inserts in case the unit must be shipped at a later date.

2. Prepare the site, including provision of a dedicated power outlet.
3. Verify that common carrier or customer-supplied DDS line is installed.
4. If you are going to use Frame Relay, obtain DLCI numbers from your carrier.
5. Obtain the console management cable from your terminal vendor. The console cable should be a straight-through cable.
6. Obtain a 10BaseT LAN cable from your local cable supplier. See Appendix C, *Interfaces and Cables*, for cables available from Osicom.
7. Obtain an IP address from your network administrator or Internet services provider.
8. If Novell IPX routing is used, obtain the IPX Network Number from your network administrator.
9. Determine the Frame Type used for IPX routing.

See page 2-7 for a summary of steps for the Quick Start Procedure.

2.2 Communications Line Requirements for CSU/DSU

The communications facility should be a DDS or metallic baseband line with a wire gauge between 19 and 26 (inclusive). The Routermate Plus will *not* operate on Dial Network (DDD) lines nor on voice-grade lines. line.

The baseband line must have the following characteristics:

- Metallic continuity
- Non-switched
- Two shielded twisted pairs
- Must not be equipped with correcting circuits, repeaters, or loading coils

We recommend that you use two separate twisted-pair cables. In noisy environments, use shielded twin cables that are grounded to your telecommunications facility.

2.2.1 FCC Part 68 Requirements for CSU/DSU

Notification to the Telephone Company

The integral 56K CSU/DSU complies with Part 68 of FCC Rules. Provide the 14-character FCC Registration Number (see multipurpose label on underside of unit), plus the Facility Interface Codes (according to data transmission speed) and Service Order Code (see frontmatter of manual) to your telephone company so they can connect the necessary service.

Malfunction of the Equipment

In the event this equipment should fail to operate properly, disconnect the unit from the communications line until you learn whether the source of trouble is in your equipment or in the line. If the trouble appears to be with this unit, discontinue use of the unit until it is repaired.

Under FCC rules, no customer is authorized to repair this equipment. This restriction applies whether the equipment is in or out of warranty.

Please note that the telephone company may ask that you disconnect this equipment from their lines until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

Incidence of Harm

If your equipment causes harm to the network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible.

Rights of the Telephone Company

Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted service.

Industry Canada's Compliance Notice

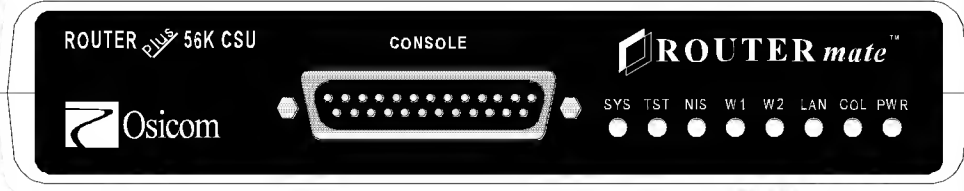
This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel du Canada.

2.3 LEDs

The table below identifies and describes the LED indicators on the front panel.

Table 2-1. LEDs		
LED	COLOR	INDICATION/FUNCTION
SYS	Red	On power-up, LED blinks momentarily, then goes out. If LED stays lighted, the unit has failed and is not operational.
	Off	Router is operational.
TST	Red	A diagnostic test is active.
NIS	Yellow	The WAN 1 interface is not in service. Out Of Sync (OOS) or Out Of Frame (OOF) received from the central office, or no signal is detected on the WAN interface.
W1	Green	The WAN interface is up.
	Off	The WAN interface is down.
W2	Green	Not used.
LAN	Green	The LAN interface is up.
	Off	The LAN interface is down.
COL	Red	Blinks once when any collision occurs on the LAN.
PWR	Green	Power is on.



2.4 Interfaces and Cables

Figure 2-1 shows the rear panel connectors.

NOTE

Do not connect cables until completing the Quick Start procedure (Section 2.6, page 2-7).

See Appendix C, *Interfaces and Cables*, for interface pin descriptions and cables available from Osicom.

WAN 1

The WAN 1 interface connects the router to the DDS Network. The connector is an RJ48, 8-pin keyed modular jack.

Use cable 115-0414-004, included with the unit, to connect the WAN 1 interface to the RJ48 Telco jack.

10BaseT

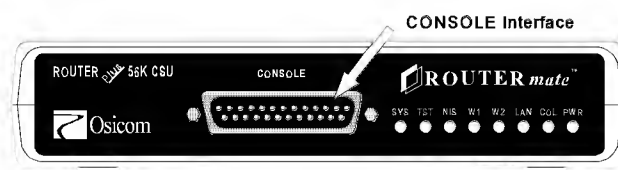
The 10BaseT Interface connects the router to the Local Area Network (LAN). It is an RJ45, 8-pin keyed modular jack. Use a customer-supplied 10BaseT drop cable to connect the **10BaseT** interface to a Media Access Unit (MAU) on the LAN.

WAN 2

When the optional integral V.32bis modem is present, this interface provides a connection to dial lines for secure remote dial-in access of the router's management screens. It is an 8-pin modular connector. See Section 2.5.4, page 2-6.

Console

The **Console** interface on the front panel is an RS-232 DB25 female connector. It provides a connection for local management via an ASCII terminal. The console cable should be a straight-through cable.



Use the terminal to access management screens for configuring, testing, and monitoring the status of the router and CSU.

Power

The Routermate Plus includes a wall-mount transformer. Refer to Table E-1, Specifications, for power requirements.

NOTE



Use only the wall-mount transformer included with the unit. See the Multipurpose Label on the underside of the unit for the part number.

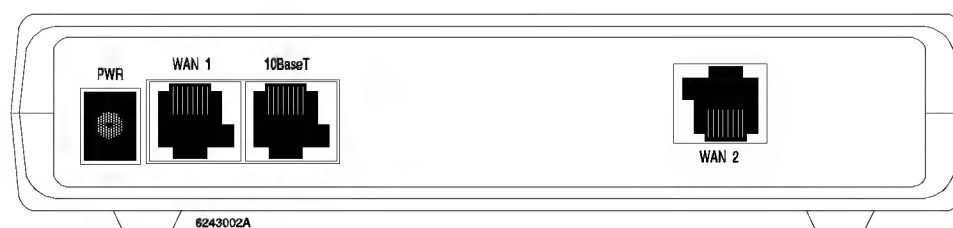


Figure 2-1. Rear Panel Connectors

2.5 Management

The Routermate Plus can be managed in a variety of ways, as follows:

- ASCII terminal
- SNMP (Simple Network Management Protocol)
- Telnet
- Dial-In management (optional)

NOTE

Before SNMP or Telnet management can be used, you must first configure the IP address on the Port IP Routing Options screen (see Quick Start Procedure, Section 2.6, page 2-7).

SNMP and Telnet can be used simultaneously; telnet and terminal management cannot.

2.5.1 Passwords

Access to certain management screens is restricted to users who can enter a password.

Either of two passwords can be entered. If neither password has been configured, enter the default password, which is **[CR]** for both passwords.

The two passwords are:

- **Console Password** - grants limited access to the management screens. The user can access all screens except encryption screens.
- **Key Password** - grants access to all screens.

Both passwords are configured on the Unit screen (see Chapter 8).

2.5.2 Terminal Management

Connect an ASCII terminal directly to the router's front-panel **CONSOLE** interface to access the management screens. See Quick Start Procedure, page 2-7.

2.5.3 Telnet/SNMP Management

Telnet allows the management screens to be accessed from any host on the network. An SNMP management station can configure the integral CSU and the optional encryption card (using the enterprise MIBs). Using the

standard MIB II, an SNMP management station can view the status of the router. See *Obtaining the Enterprise MIB*, Section 2.7, page 2-10.

Telnet or SNMP management can be performed via the LAN or WAN interface. To manage the Routermate Plus using Telnet or SNMP:

1. IP routing must be enabled (default). See IP Routing Options in Chapter 5).
2. If the WAN interface is configured for *Unnumbered* mode (default), you must use the LAN IP address (default is 192.0.2.1).
3. If the WAN interface is configured for *Numbered* mode, you can use either the LAN or WAN IP address (default WAN address is 192.0.3.1).
4. Verify that the interface associated with the address you are attempting to access is *Up* (see the LAN Status and WAN Status screens in Chapter 4).
5. For SNMP management, configure the **SNMP R/O Community** and the **SNMP R/W Community** to match the strings used by the SNMP management station (see the Management screen in Chapter 9).

Defaults: R/O = *public*
R/W = *private*

6. For Telnet access, set the **Telnet Server** parameter on the Management screen to *Enabled* (default).

After making a Telnet connection to a defaulted unit, configure the IP addresses assigned by your network administrator to the router's LAN port. When you re-configure the IP address for the interface to which the Telnet session is connected, the Telnet session is interrupted. You can then establish a new connection, if you wish, to the newly configured address.

NOTE

The default IP addresses are only to facilitate initial configuration by remote access. They cannot be used as the permanent IP addresses.

2.5.4 Dial-In Management

This optional feature provides a backup management path. The optional **WAN 2** interface is used for secure dial-in management. A remote modem operator can access the terminal management screens. The remote modem must be V.32-compatible.

Before making a dial-in management call, attach the cable and configure the integral and originating modems as follows:

1. Connect the DDD line cable (115-0414-001) from the **WAN 2** interface to an RJ11 jack.
2. On the Modem screen (see Chapter 7), configure the following parameters:
 - **Modem Security** (default = Disabled)
 - **Security Password** (default = *password*)
 - **Auto Answer** (default = Enabled)

NOTE

If using Osicom's 4532 or 4232 modem, you can enable **Modem Security** to prevent an unauthorized connection. If using a modem other than Osicom's 4532 or 4232 modem, **Modem Security** must be disabled.

3. If using Osicom's 4532 or 4232 modem to originate the call, configure the originating modem as follows:

- a. Enable level 1 security.

AT"E1

- b. Set both passwords to match the **Security Password** (default is *password*).

AT"Zpassword

AT"Ypassword

- c. Set the modem user ID to usr in order to connect the router with security. Use AT"Wusr.

After making a connection, enter any key; the router's banner screen appears and you are prompted to enter a terminal selection, followed by the password.

2.6 Quick Start Procedure

The following steps facilitate initial installation and configuration.

NOTE

This procedure assumes you are accessing the management screens from a directly-connected terminal.

Before starting the procedure, verify that the items in the Installation Checklist (page 2-1) have been completed.

If you encounter any problems or have any questions during installation, contact Osicom Technologies' Customer Service Department at (800) 359-2273.

See Chapter 5, *Configuration*, for detailed descriptions of operational parameters.

Default settings - The default settings allow you to get started quickly and easily with minimal configuration.

If your application matches the default settings of IP routing over an unnumbered PPP link, then you only need to configure the CSU and assign DS0s (step 3) and configure the IP address and subnet mask on the LAN port (step 6).

The default settings are:

LAN interface:

Protocol: *Ethernet (fixed)*

Port 0 (LAN):

IP Address: 192.0.2.1
Subnet Mask: 255.255.255.0
IP Routing: *Enabled*
IPX Routing: *Disabled*
Bridging: *Disabled*

WAN Interface:

Protocol: *PPP (Point-to-Point)*

Port 1 (WAN):

IP Routing: *Enabled*
Mode: *Unnumbered*
IPX Routing: *Disabled*
Bridging: *Disabled*

Port 1 IP Address: 192.0.3.1 (Numbered Mode)
Subnet Mask: 255.255.255.0

Perform all the steps in the procedure if your application requires settings that are different from those above.

Summary of Steps:

1. Apply power to router.
2. Connect terminal.
3. Configure CSU.
4. Select WAN protocol; PPP or Frame Relay.
5. Enable or disable IP, IPX, Bridging for the LAN port (Port 0).
6. Configure IP, IPX options for the LAN port.
7. Enable or disable IP, IPX, Bridging for the WAN port(s).
8. Configure IP, IPX options for the WAN port(s).
9. Save configuration to Flash.
10. Connect LAN and WAN cables.

STEP 1 - Power Up

1. To apply power insert the power cord into the connector labeled **PWR**, then plug the wall-mount transformer into a dedicated outlet.
2. The red **SYS** LED blinks momentarily during power-up, then goes out.

If the **SYS** LED stays on, the unit has failed and is not operational. Disconnect and then re-connect the power cord. If the unit fails again, contact your dealer or Osicom Technologies.

STEP 2 - Connect Terminal

1. Use a straight-through RS-232 cable to connect a VT100-compatible terminal to the **CONSOLE** port on the front of the router. Power-on the terminal and configure the terminal as follows:

Rate: 9600 bps Parity: none
Mode: full duplex Stop bits: 1
Character: 8 bits CR = CR
Flow control: C1/DC3 (Xon/Xoff)

2. The Terminal Selection screen appears. If the Terminal Selection screen does not appear, type **[CTRL-N]**.
3. Type the letter for the type of terminal that is connected to the router; you are prompted for a password.
4. Type **[CR]**, the default password, to access the management screens. The Main Menu is displayed.

If the terminal displays garbled characters, press **[Ctrl-N]** to return to the Terminal Selection screen, where you can select a different terminal type.

STEP 3 - Configure the CSU

Access the CSU Configuration screen and configure the following parameter:

Timing - Repeater (default)

STEP 4 - Configure Protocol for the WAN Interface

1. Access the **WAN 1 Configuration** screen.
2. Select the **Protocol**: *PPP* (default), *Frame Relay - Annex D*, or *Frame Relay - No LMI*.

STEP 5 - Enable, disable IP, IPX, Bridging for the LAN Port (Port 0)

1. Access the **Port 0 Configuration** screen and set **IP Routing**, **IPX Routing**, and **Bridging** to *Enabled* or *Disabled*.

STEP 6 - Configure IP, IPX Options for the LAN Port (Port 0)

If IP Routing is *Enabled*:

1. Access the **Port 0 IP Routing Options** screen.
2. Configure the **Address** (32-bit IP address). (Default = 192.0.2.1)
3. If IP subnetworking is used, configure the **Subnet Mask** provided by your network administrator.
4. Configure **Frame Type** to match the type used on the LAN. The default is TYPE II, which is almost always used.

If IPX Routing is *Enabled*:

1. Access the **Port 0 IPX Routing Options** screen.
2. Configure the **IPX Network Number** for the LAN.
3. Configure the **Frame Type** to match the type used on the LAN.

STEP 7 - Enable, Disable IP, IPX, Bridging for WAN Ports

For Point-to-Point applications, configure the following for Port 1 only.

For Frame Relay applications, configure the following for each port 1-14 as required.

1. Access the **Port Configuration** screen.
2. Set **IP Routing**, **IPX Routing**, and **Bridging** to *Enabled* or *Disabled*.
3. *Frame Relay only*: Configure **DLCI** to the DLCI for this port. **The number configured here is the DLCI used to reach the remote site.**
4. *Frame Relay only*: verify **Encapsulation** is set for RFC1490 (default).

STEP 8 - Configure IP, IPX Options for WAN Port(s)

For Point-to-Point applications, configure the following for Port 1.

For Frame Relay applications, configure the following for each port for which a DLCI was configured in the previous step.

If IP Routing is Enabled:

1. Access the **IP Routing Options** screen for the individual port.
2. Configure the **IP Address** and **Subnet Mask**. No entries are required for Unnumbered Mode.

For Frame Relay applications:

If the remote router requires it, enable **Inverse ARP** on the port IP Routing Options screen. The Routermate Plus does not require Inverse ARP (default is disabled).

If IPX Routing is Enabled:

1. Access the **IPX Routing Options** screen for the individual port.
2. Configure the **IPX Network Number** for the WAN. No entries are required for Unnumbered Mode.
3. Enable or Disable **IPXWAN** to match the router on the other end of the WAN link. Support for IPXWAN is only provided to allow the router to be compatible with Novell routers. It is not required to route IPX and should be disabled unless it is required. The default is disabled.

For Frame Relay applications:

If the remote router requires it, enable **Inverse ARP** on the port IPX Routing Options screen. The Routermate Plus does not require Inverse ARP (default is disabled).

STEP 9 - Save Configuration to Flash

When your configuration has been implemented and checked out to be satisfactory, return to the Main Menu and select **Save to Flash**; a prompt will appear to confirm your selection.

If the new configuration is not satisfactory, power cycle the router (off-on) before saving it to restore the original configuration.

STEP 10 - Attach LAN and WAN Cables

1. Use cable 115-0414-004, included with the unit, to connect the **WAN 1** interface to the network.
2. Use a customer-supplied 10BaseT drop cable to connect the **10BaseT** interface to the LAN.

You are now ready to pass data. Refer to the following chapters for detailed information on configuration and management screens.

- Chapter 5: *Configuration*
- Chapter 8: *Unit Configuration*
- Chapter 9: *Management Configuration*

2.7 Obtaining the Enterprise MIB

There are two enterprise MIBs:

- CSU - configure and monitor CSU parameters.
- Encryption - configure encryption options.

The enterprise MIB can be downloaded from Osicom's Web site at: osicom.com.

This chapter provides an overview of terminal management. After reading this chapter, the user will be familiar with the following:

- Terminal screen structure and hierarchy of menus
- Keys, conventions, and screen paths - which keys to use to move around screens, edit parameters, and access other screens
- ASCII terminal communication parameters
- Terminal Selection
- Password
- Main Menu
- Save To Flash
- Logoff procedure

3.1	Screen Structure	3-1
3.2	Keys and Conventions	3-2
3.3	Terminal Selection	3-3
3.4	Password	3-4
3.5	Main Menu	3-5
3.5.1	Save To Flash	3-5
3.5.2	Logoff	3-5
3.5.3	Screen Path	3-5

3.1 Screen Structure

Figure 3-1 shows the screen structure for the Routermate Plus.

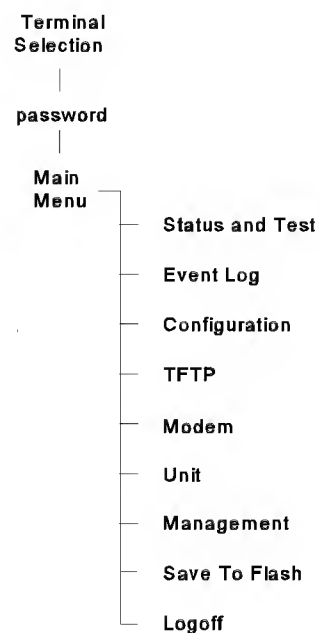


Figure 3-1. Screen Structure

3.2 Keys and Conventions

Prompts at the bottom of each screen instruct the user which keys to use to:

- Position the cursor
- Edit parameters
- Execute commands
- Access other screens

Table 3-1 summarizes the most frequently used keys.

Edit Fields

To configure a parameter by typing a value:

- Press **[CR]** to highlight the field.
- Type the value.
- Press **[CR]** again to exit the field.

To restore the parameter to its original contents, press **[Esc]** before exiting the field.

To edit existing text in a field that can be edited:

- Move the cursor to the field and press **[Ctrl-E]** to highlight the field.
- Use the arrow keys to move the cursor within the field.
- Type over the existing information.
- Press **[CR]** to exit the field.

To delete existing text from a field that can be edited:

- Move the cursor to the field and press **[CR]**.
- Press **[Space Bar]**.
- Press **[CR]** again.

Selecting from multiple options

- Move the cursor to the parameter.
- Press **[CR]** to toggle/scroll through the available options.
- When the desired option is displayed, either move the cursor to the next parameter using **[Space Bar]** or **[Backspace]**, or exit the screen.

To restore the parameter to its original contents, press **[Esc]** before exiting the field.

Saving Changes

Press **[X]** to exit from a screen. If you have modified any parameter, you are prompted:

Confirm this configuration?
No Yes

Select *No* to exit the current screen without saving the changes; select *Yes* to save the changes and exit.

Table 3-1. Frequently Used Keys	
KEY	FUNCTION
Move Around in Screens	
[Space Bar]	cursor down
[Back Space]	cursor up
[Ctrl-N]	Terminal Selection screen
[Ctrl-O]	re-draw screen
[Ctrl-T]	return to Main Menu *
[X]	exit to previous screen
Type an Entry	
[CR]	select field
[Back Space]	delete character left
[Esc]	restore original setting
[Ctrl-E]	highlight field, edit text
[CR][Space Bar][CR]	delete current contents
Select From List	
[CR]	scroll/toggle through list
[Esc]	restore edited field to original setting
[Space Bar]	move to next field
* [Ctrl-T] returns to the Main Menu <u>without</u> prompting to confirm configuration changes.	

Certain prompts will change to correspond to the function or operation. An example is shown below.

FUNCTION/OPERATION	PROMPT
Edit an entry	Edit Field = [CR]
Select from multiple options	Scroll Through Options = [CR]
Select another menu	Select Menu = [CR]

3.5 Main Menu

The Main Menu is the top level screen from which you select other screens to manage and configure the router.

To make a selection from the Main Menu:

1. Press **[Space Bar]** or **[Back Space]** to move the cursor to the desired selection.
2. Press **[CR]**; the selected menu appears.

3.5.1 Save To Flash

After the current configuration checks out to be satisfactory, you can save it to Flash as the permanent configuration. To save the current configuration to flash:

1. Position the cursor on **Save To Flash**.
2. Press **[CR]**; a message box is displayed indicating the status of save.

If *Yes* is selected, "Saving Configuration, please wait" is displayed, followed by "Save to flash complete" with the cursor next to a choice of *OK*.

While "Saving Configuration, please wait" is displayed, keyboard input is ignored.

3.5.2 Logoff

Select **Logoff** to return to the Terminal Selection screen. Access to the management screens is then restricted to users who can enter either the console password or the key password.

NOTE

Configuration changes are lost if the unit is reset or power is turned off without first saving the configuration to flash.

3.5.3 Screen Path

To help the user navigate through the menus and screens, a **Screen Path** is illustrated next to each screen. Screen names are inside boxes. Commands and on-screen selections that lead to a screen are written in *italics*.

In the example below: at the Terminal Selection screen, enter the terminal selection **[A - F]** to display the Password screen. Enter the password to display the Main Menu.

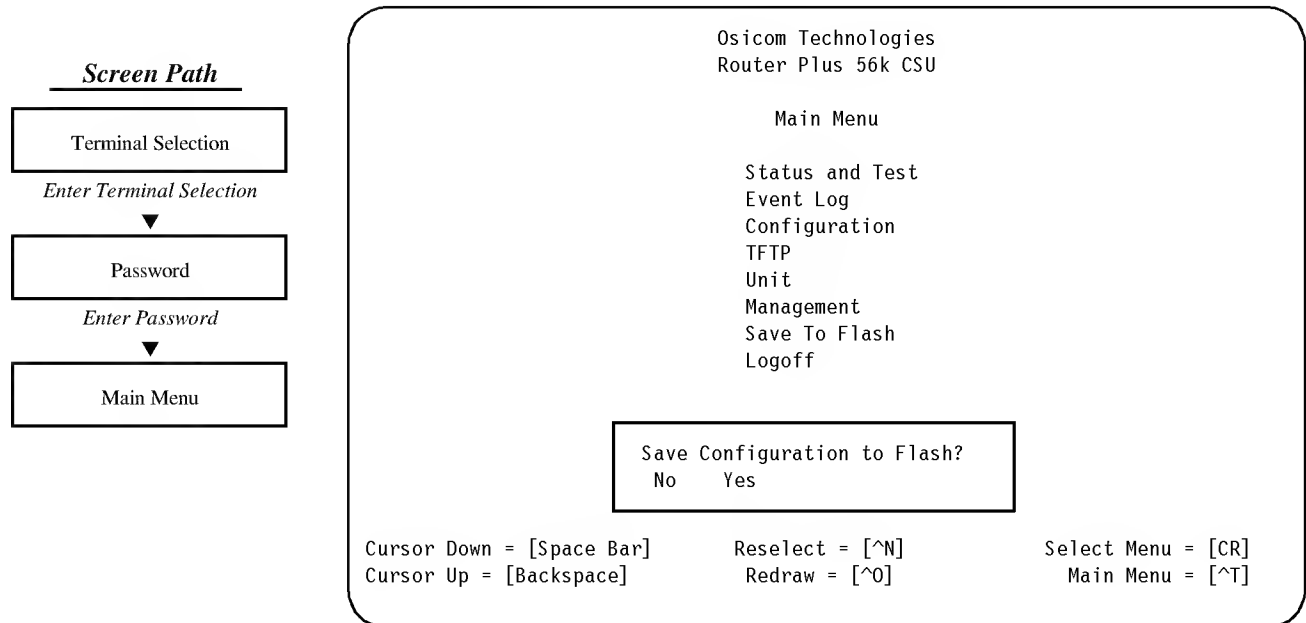


Figure 3-4. Main Menu

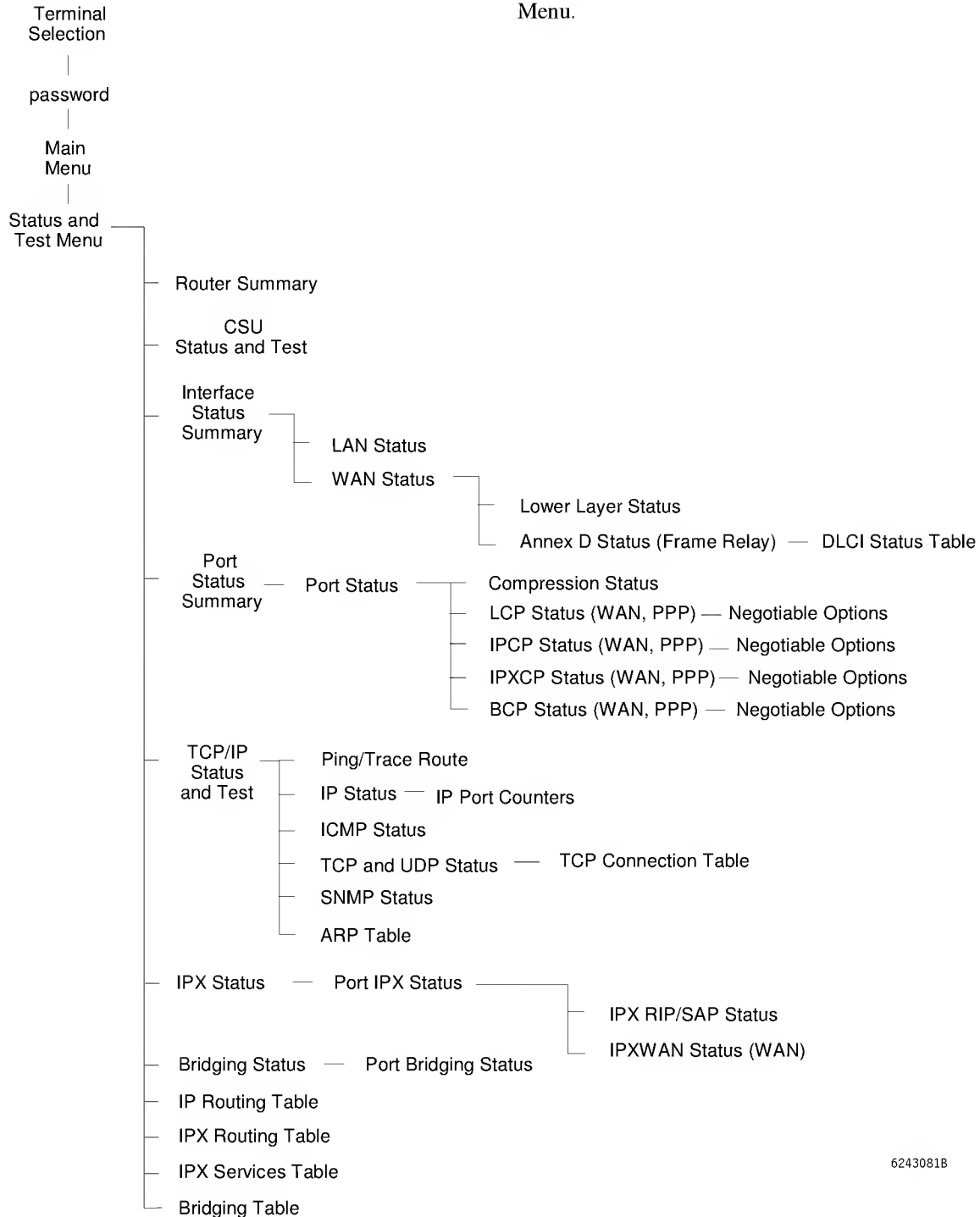
This chapter illustrates and describes the router's status and test screens and the event log. Basically, this text serves as a reference tool for defining the various parameters and options appearing on the screens.

After reading this chapter, the user will be able to locate specific interface and port status and test screens and understand the contents and purpose of each.

4.1	Screen Structure	4-2
4.2	Status and Test Menu	4-5
4.3	Router Summary	4-6
4.4	CSU Status and Test	4-8
4.4.1	Loopback Tests	4-8
4.4.2	Line Status	4-9
4.5	Interface Status Summary	4-10
4.5.1	LAN Status	4-11
4.5.2	WAN Status (Frame Relay)	4-13
4.5.2.1	Lower Layer Status (WAN)	4-14
4.5.2.2	Annex D Status	4-15
4.5.2.2.1	DLCI Status Table	4-16
4.5.3	WAN Status (PPP)	4-17
4.6	Port Status Summary	4-18
4.6.1	Port Status (LAN - Ethernet) ...	4-19
4.6.2	Port Status (WAN, Frame Relay) ..	4-20
4.6.3	Port Status (WAN, PPP)	4-21
4.6.3.1	LCP Status	4-22
4.6.3.1.1	LCP Negotiable Options	4-24
4.6.3.2	IPCP Status	4-25
4.6.3.3	IPXCP Status	4-26
4.6.3.4	BCP Status	4-27
4.7	TCP/IP Status and Test Menu ..	4-28
4.7.1	Ping/Trace Route	4-28
4.7.2	IP Status	4-30
4.7.2.1	IP Port Counters	4-32
4.7.3	ICMP Status	4-33
4.7.4	TCP and UDP Status	4-34
4.7.4.1	TCP Connection Table	4-36
4.7.5	SNMP Status	4-37
4.7.6	ARP Table	4-39
4.8	IPX Status	4-40
4.8.1	IPX Status (LAN and WAN) ...	4-41
4.8.1.1	IPX RIP/SAP Status (LAN and WAN)	4-43
4.8.1.2	IPXWAN Status	4-44
4.9	Bridging Status	4-45
4.9.1	Port Bridging Status	4-46
4.10	IP Routing Table	4-47
4.11	IPX Routing Table	4-49
4.12	IPX Services Table	4-51
4.13	Bridging Table	4-52
4.14	Event Log	4-53

4.1 Screen Structure

The organization of the **Status and Test** screens is shown below. Access the Event Log from the Main Menu.



6243081B

Figure 4-1. Screen Structure (Status and Test)

The Status and Test screens and the Event Log are described below.

Router Summary - view the major configured options and parameters of all the ports defined on the router, including: interface, operational status, DLCI (frame relay), IP address, IPX network number, and bridging status.

CSU Status and Test - initiate and monitor loopback tests and monitor alarm conditions for the integral CSU.

Interface Status Summary - view the configured protocol for the LAN and WAN interfaces and the operational status of each. Access the interface-specific screens below.

LAN Status - view the configured and operational condition of the LAN interface; monitor counters and statistics.

WAN Status - view the configured and operational condition of the WAN interface; monitor counters and statistics; access the screens below.

Lower Layer Status - monitor statistics of errored frames transmitted and received over the WAN interface; monitor WAN utilization.

Annex D Status (Frame Relay only) - monitor RFC 1315 error and status messages; access the DLCI Status Table.

DLCI Status Table (Frame Relay only)
- view the status of all configured Data Link Connection Identifiers (DLCIs).

Port Status Summary - view the status of all the virtual ports configured on the router; includes port name, corresponding interface, protocol, and condition (up, down, or disabled). Access the port-specific status screens below.

Port Status (LAN) - view the status and monitor counters and statistics for the LAN interface.

Port Status (WAN) - view the status and monitor counters and statistics for each port on the WAN interface. If the protocol is PPP, access the screens below.

LCP Status (PPP only) - view the status of the Link Control Protocol, which is used to configure, maintain, and terminate a point-to-point link.

LCP Negotiable Options - view the values of LCP negotiable options in configuration requests sent and received by the router.

IPCP Status (PPP only) - view the status of the IP Control Protocol, which is responsible for configuring and establishing the PPP IP protocol modules on both ends of a point-to-point link.

IPXCP Status (PPP only) - view the status of the IPX Control Protocol, which is responsible for configuring and establishing the PPP IPX (Internetwork Packet eXchange) protocol modules on both ends of a point-to-point link.

BCP Status (PPP only) - view the status of the Bridging Control Protocol, which is responsible for configuring and establishing the PPP bridge protocol modules on both ends of a point-to-point link.

TCP/IP Status - access the screens below.

Ping/Trace Route - use the ping command to determine if a gateway (router) or host in the network is reachable or use the trace route command to determine the routes used from your router to a specified host or gateway (router).

IP Status - view information and statistics for the Internet Protocol (IP) for all ports on the router which are configured for IP routing.

IP Port Counters - view the number of datagrams received and transmitted each port configured for IP routing.

ICMP Status - view information and statistics for the Internetwork Control Message Protocol (ICMP) for all ports on the router which are configured for IP routing.

TCP and UDP Status - view information and statistics for the TCP (Transmission Control Protocol) and UDP (User Data Protocol) for all ports on the router which are configured for IP routing; access the screens below.

TCP Connection Table - view MIB II information about the router's existing TCP connections.

SNMP Status - view input and output statistics and counters for Simple Network Management Protocol.

ARP Table - view the physical address and corresponding network address used in Address Resolution Protocol.

IPX Status - view a summary of information and statistics for all ports on which IPX (Internetwork Packet eXchange) routing has been enabled; access the screens below.

Port IPX Status (LAN and WAN) - view information and statistics of each ports on which IPX routing has been enabled.

Port IPX RIP/SAP Status (LAN and WAN) - view input and output RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) message counters.

Port IPXWAN Status (WAN only) - view the status of counters for IPXWAN protocol, which is used for establishing connections across point-to-point (WAN) links.

Bridging Status - view a summary of information and statistics for each port on which bridging is enabled; access the port-specific screens.

Port Bridging Status - view counters for various types of received and transmitted frames.

IP Routing Table - view the IP Routing Table.

IPX Routing Table - view the IPX Routing Table.

IPX Services Table - view the Service Advertising Protocol (SAP) Table. SAP is an IPX protocol that is used to advertize various Novell application services offered by such devices as file servers, printer servers, and gateways.

Bridging Table - view the Bridging Table.

Event Log - view network messages that occur during startup and operation of the router.

4.2 Status and Test Menu

Access the Status and Test Menu (Figure 4-2) from the Main Menu. This is the top-level menu from which you select other screens to run diagnostic loopbacks on the CSU and view the status and statistics of the LAN and WAN interfaces.

To make a selection:

1. Press **[Space Bar]** or **[Back Space]** to move the cursor to the desired selection.
2. Press **[CR]**; the selected menu appears.

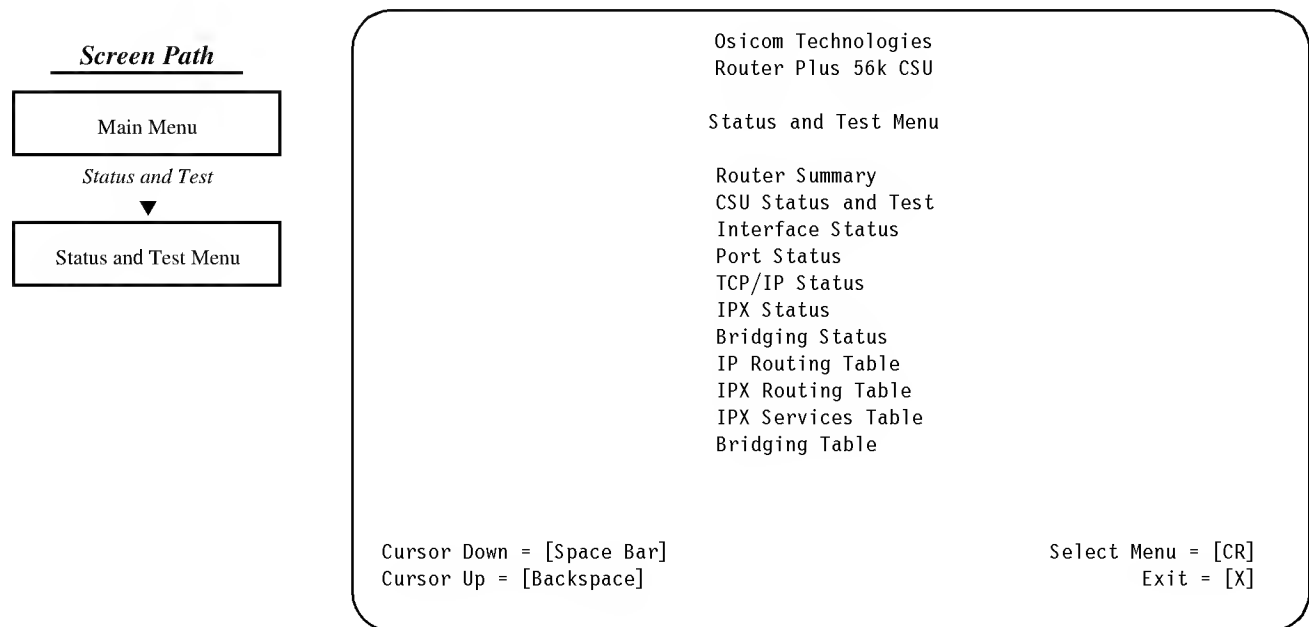


Figure 4-2. Status and Test Menu

4.3 Router Summary

The Router Summary screen provides an informational and operational status report on all the ports configured on the router. You can view the status of up to 15 logical ports configured. Figure 4-3 illustrates a Frame Relay application and Figure 4-4 illustrates a PPP application.

Port 0 is always assigned to the LAN interface and ports 1 through 14 are available for the WAN interface.

This screen is updated every two seconds.

The MAC address is permanently displayed in upper left corner of the screen.

Port - identifies the port number and the first 8 characters of the port name.

Interface - identifies the interface (LAN or WAN 1) to which the port is configured and whether the interface is *Up*, *Down*, or *Dis* (Disabled).

DLCI/PPP - identifies the Data Link Connection Identifier or Point-to-Point NCP (Network Communications Protocol) status. This field is blank for LAN.

Frame Relay: the DLCI number and (*Up*, *Down*, or *Dis* (Disabled)).

PPP: Any NCPs that are up are displayed (in the example shown in Figure 4-4, IP and IPX are up). NCPs that are not up are not displayed.

IP Address - Internet protocol enabled (Y) or disabled (N) and local IP address assigned to the port.

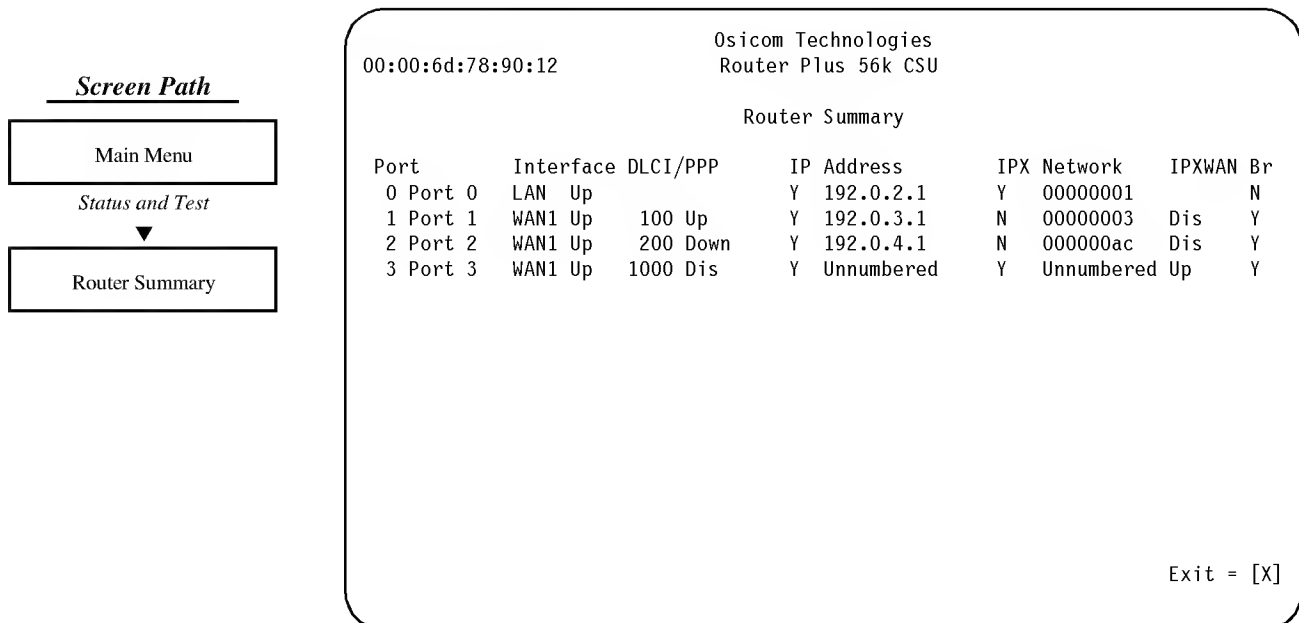


Figure 4-3. Router Summary (Frame Relay)

IP Address and IPX Network - the IP Address and the IPX Network fields display Unnumbered when a WAN port set to Unnumbered. If IPXWAN is enabled, the network number may be a number assigned by IPXWAN instead of the number configured for the port. IPXWAN assigns the primary network number based on the master/slave relationship. If the local and remote router's WAN ports have different IPX network numbers, then the master unit will assign an IPX network number to the slave.

(Y) is protocol enabled; (N) is disabled.

IPXWAN - IPXWAN status: *Up, Down, or Disabled.* (WAN only) - a protocol developed by Novell and specified in RFC1634. The purpose of IPXWAN is to provide a common way of exchanging router to router information across different type of wide area links. RFC1634 describes how Novell IPX operates over various WAN media using the IPXWAN protocol.

Support for IPXWAN is only provided to allow the router to be compatible with Novell routers. It is not required to route IPX and should be disabled unless it is required. The default is disabled.

NOTE

IPXWAN must be set to the same value on both ends of a connection. If it is not set to the same value, then the router will not be able to communicate across the link.

Br - bridging enabled (Y) or disabled (N).

Screen Path

Main Menu

Status and Test

▼

Router Summary

00:00:6d:78:90:10

Osicom Technologies
 Router Plus 56k CSU

Router Summary

Port	Interface	DLCI/PPP	IP Address	IPX Network	IPXWAN	Br
0 Port 0	LAN	Up	Y 192.0.2.1	Y 00000001		N
1 Port 1	WAN1	Up IP	Y 192.0.3.1	Y 00000003	Dis	N

Exit = [X]

Figure 4-4. Router Summary (PPP)

4.4 CSU Status and Test

Use the CSU Status and Test screen (Figure 4-5) to start and monitor loopback tests, view test counters, and observe the line status. This screen is updated every two seconds.

Press **[C]** to clear the **Seconds In Test** and **Seconds In Error** counters. These counters are also cleared when a test is selected.

Loopback states are shown in two columns that correspond to the SNMP 'admin' and 'state' equivalents.

On or *Off* (admin) – set by the user to indicate the desired state of the loopback test.

Yes or *No* (state) – indicates the actual state of the loopback test.

When a test is set to *On* and has responded, the 'state' column indicates *Yes*. *Off - Yes* indicates that the loopback was set by the remote unit.

NOTE - SNMP Management

Do not start a test that will disconnect the communications path between the router and the SNMP manager.

4.4.1 Loopback Tests

Local Loop + Test Pattern - a CSU local loop and test pattern generator for local testing. The CSU automatically transmits a pseudo random 511 test pattern that is looped back to the receiver and checked for errors. Observe the counters for Seconds in Test and Seconds In Error.

Remote Digital + Test Pattern - the local CSU sends a loop up test to the remote CSU that causes the remote CSU to enter Digital Loop.

NOTE

If in LDM mode, only the end set to *Internal* timing can initiate this test.

Digital Loop - the CSU enters a unidirectional loopback. Data received from the network is retransmitted back out the active interface. Observe the counters for Seconds in Test and Seconds In Error.

NOTE

This test can only be initiated by a unit set to *Repeater* timing.

Screen Path

Status and Test Menu

CSU Status and Test



CSU Status and Test

```

Osicom Technologies
Router Plus 56k CSU

CSU Status and Test

Local Loop + Test Pattern:      Off - No
Remote Digital + Test Pattern:  Off - No
Digital Loop:                   Off - No
Test Pattern                    Off - No
Remote End of Remote Digital Loop: No

Seconds In Test:                999999
Seconds In Error:               999999

Not In Service:                 000000

Line Status:                    00S/00F

Cursor Down = [Space Bar]      Select = [CR]
Cursor Up   = [Backspace]      Exit   = [X]
Clear       = [C]
  
```

Figure 4-5. CSU Status and Test

Test Pattern - a test pattern generator/comparator that sends a test pattern out the WAN interface. The test pattern generated is a pseudo random 511 pattern. External test sets can be connected to a CSU/DSU at the remote end to monitor the transmitted data. The test set can also send data to the CSU which checks the received pattern for errors. Errors are reported on the counters.

Remote End Of Remote Digital Loop - not selectable. The 'state' column (Yes/No) indicates the condition of the loopback at the remote end.

Seconds In Test - length of time the Test Pattern has been enabled.

Valid range: 0 to 999999 seconds.

Seconds In Error - the number of seconds that contained an error.

Valid range: 0 to 999999 seconds.

Not In Service - the number of times a Not in Service signal was detected. This includes No Signal, OOF (Out Of Frame), and OOS (Out Of Service).

4.4.2 Line Status

One or more of the following CSU/DSU Line Status messages can appear, depending on current operating conditions.

Data Mode - the CSU is receiving user's data from the remote unit.

Idle - the DDS line is active but no data is being received.

No Signal - no inbound signal detected for more than 32 clock cycles (0.8 mS at 56,000 bps).

OOS/OOF - the CSU is receiving the Out-of-Service (OOS) or Out-of-Frame (OOF) signal from the Telco.

CSU Loop - a test initiated by the Telco at the user's request. A polarity reversal of the sealing current on the Telco line causes a loopback through the CSU section of the unit.

DSU Loop - a test initiated by the Telco at your request. An inband test pattern sent by the Telco causes a loopback similar to the Digital Loop to occur.

4.5 Interface Status Summary

Access the Interface Status Summary screen (Figure 4-6) to view the condition of the LAN and WAN interfaces.

See WAN Configuration in Chapter 5 for descriptions of protocols.

Interface status corresponds to MIB II Interface operational state.

This screen is updated every two seconds.

Interface Status		
PROTOCOL	STATUS	CONDITION
Ethernet	Up Down Disabled	Link is up Link is down Interface State set to disabled
PPP (Point-to-Point)	Up Down Disabled	The LCP (Link Control Protocol) is up The LCP is not up Interface State set to disabled
FR-No LMI (Local Management Interface)	Up Down Disabled	Flags are present and CSU Line Status is up Flags are missing or CSU Line Status is down or in test Interface State set to disabled
FR-Annex D	Up Down Disabled	Network is responding to LMI request * Network is <u>not</u> responding to LMI request * Interface State set to disabled
* Determined by Error Threshold option (see WAN protocol options for Frame Relay in Chapter 5).		

Screen Path

Status and Test Menu

Interface Status

▼

Interface Status Summary

Osicom Technologies
Router Plus 56k CSU

Interface Status Summary

Interface	Protocol	Status
LAN	Ethernet	Up
WAN 1	FR - Annex D	Up

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Select Menu = [CR]
Exit = [X]

Figure 4-6. Interface Status Summary

4.5.1 LAN Status

Access the LAN Status screen (Figure 4-7) to view the operational condition of the LAN interface. The protocol for the LAN interface is fixed at Ethernet. This screen is updated every two seconds.

Press **[C]** to clear all counters.

The counters are based on MIB II RFC 1213.

Protocol - the configured protocol for the LAN interface. Fixed at Ethernet.

State - the configured state (Enabled/Disabled) of the LAN interface.

Status - the operational status (Up/Down) of the LAN interface.

System Up Time - the amount of time the unit has been operational (days:hours:minutes:seconds).

Last Change - the system up time value when the interface entered its current operational state.

Link Downs - number of times the LAN interface has entered the link down state.

Octets - number of octets (bytes) in each frame, including the Ethernet header, but excluding the CRC.

Unicast Packets - Input: all frames received from the ethernet chip including any frames containing unknown protocols (frames received in error are not counted). When bridging is disabled, only received frames with the ethernet chip's MAC address are counted; when bridging is enabled, all frames on the LAN are counted. **Output:** all frames transmitted to the ethernet chip including all bridged, routed, and frames sourced by the router.

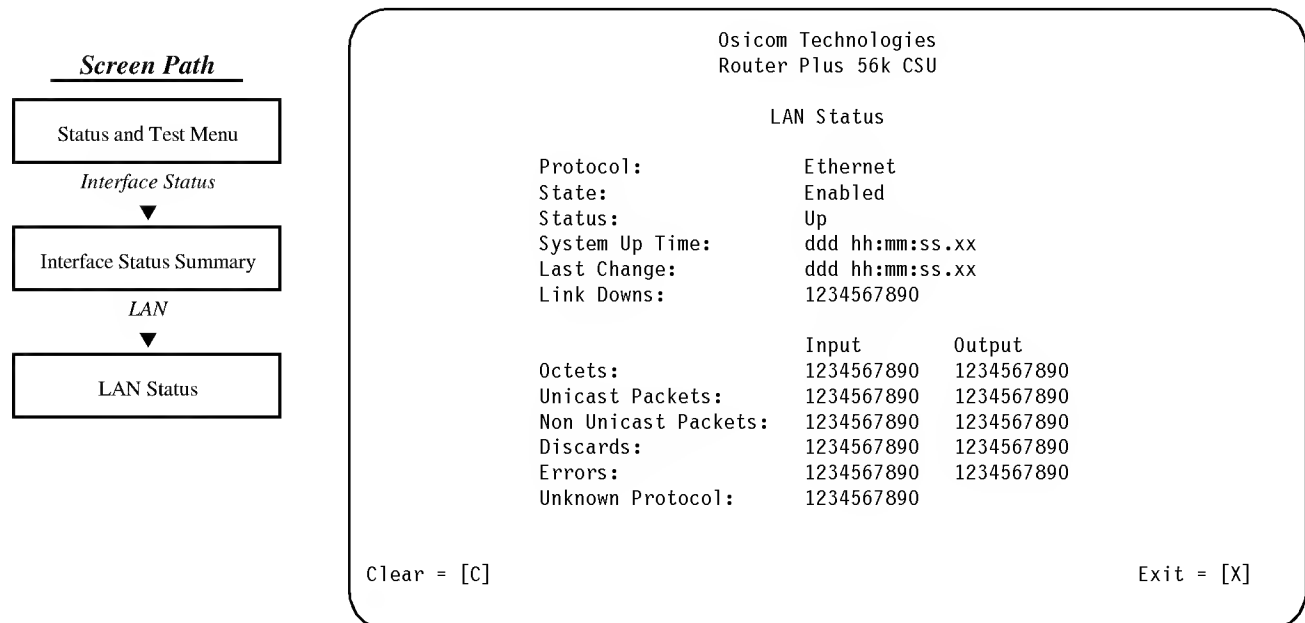


Figure 4-7. LAN Status

Non Unicast Packets - number of subnetwork broadcast (all destinations) or multicast (multiple destination) packets received (input) or to be transmitted (output) on the LAN interface, including those that were discarded or not sent.

Discards - **Input:** number of error-free frames received that could not be forwarded because of no buffer space. **Output:** number of frames that the router or bridge could not forward because of no buffer space.

Errors - **Input:** the total number of Ethernet frames received in error. These errors are detected by the Ethernet chip and cause the appropriate input error counter on the LAN Port status screen to increment. Frames containing errors are not passed up to a higher layer protocol. **Output:** the total number of Ethernet frames that an error occurred while transmitting. These errors are detected by the Ethernet chip and also cause the appropriate output error counter on the LAN Port status screen to increment.

Unknown Protocol (Input only) - the total number of frames received with the Ethernet protocol field set to a protocol that is not supported or is not enabled. Supported protocol field values are IP and IPX. The protocol field is checked for the encapsulation types selected on the IP and IPX routing options screen. Note that IP and IPX can be set to different encapsulation types which requires the Unknown Protocol test to be performed in both encapsulation types. The Unknown Protocol test is not performed on bridged frames. Frames containing Unknown Protocols are not passed up to a higher layer protocol.

4.5.2 WAN Status (Frame Relay)

Use the WAN status screen (Figure 4-8) to view statistical information for the WAN link. Annex D Status is available only if the protocol on the WAN Configuration screen is set for FR – Annex D. This screen is updated every two seconds.

See LAN Status in the previous section for parameters and counters not defined here.

The counters are based on MIB II RFC 1213.

Press **[C]** to clear all counters.

Protocol - the configured protocol for the WAN interface.

Status -

Annex D (Determined by Error Threshold option)

Up - Network is responding to LMI request.

Down - Network is not responding to LMI request.

No LMI

Up - flags are present and CSU Line Status is UP.

Down - flags are missing or CSU Line Status is down or in test.

Octets - Input: number of octets (bytes) in each received frame, including the DLCI address and control fields, but excluding the CRC. The value reported by the SCC (Serial Communications Controller) includes the CRC but the CRC octets are subtracted before the counter increments.

Output: all bytes in each frame transmitted to the SCC including the DLCI address and control fields, but excluding the CRC (the CRC is added after the frame is counted or sent).

Unicast Packets - Input: all frames received from the SCC including LMI frames. **Output:** all frames transmitted to the SCC including LMI frames.

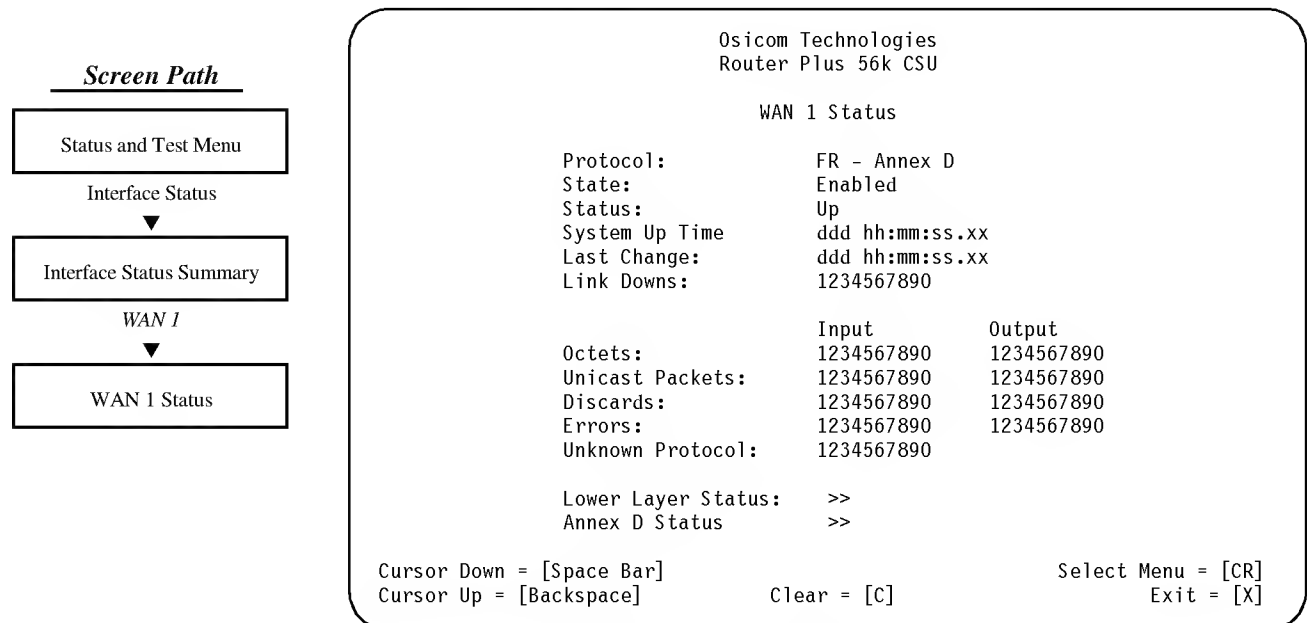


Figure 4-8. WAN 1 Status (Frame Relay)

Errors - Input: the total number of frames received in error. This includes any frames received with HDLC errors. HDLC errors (CRC, aborts, overruns, and too longs) are detected by the SCC and cause the appropriate error counter on the Lower Layer screen to increment. Frames containing errors are not passed up to a higher layer protocol. **Output:** the total number of frames that an error occurred while transmitting. These errors are detected by the SCC and also cause the Underrun counter on the Lower Layer screen to increment

Unknown Protocol - the total number of frames received with Frame Relay protocol field set to a protocol that is not supported or is not enabled. Supported Frame Relay NLPID/PID field values are LMI, IP, IPX, and bridging. Frames containing Unknown Protocols are not passed up to a higher layer protocol.

4.5.2.1 Lower Layer Status (WAN)

Figure 4-9 illustrates the Lower Layer Status screen for the WAN interface. Use this screen to monitor statistics of errored frames transmitted and received over the WAN interface and also monitor WAN utilization. The screen shown is displayed if the protocol is PPP. This screen is updated every two seconds.

Incrementing any of these error counters also causes the Input Errors or Output Errors counters to increment on the Interface Status screen.

CRC Errors - received frames detected by the Serial Communications Controller (SCC) that contained HDLC Cyclic Redundancy Check (CRC) errors

Aborts - aborted received frames detected by the SCC.

Too Longs - HDLC frames received that exceeded the maximum permitted frame size. The WAN interface can accept frames up to 2048 bytes long.

Overruns - received overrun frames reported by the SCC.

Underruns - transmitted underrun frames reported by the SCC.

Utilization - percent usage of available WAN link bandwidth during, as indicated, either 2 seconds or 60 seconds.

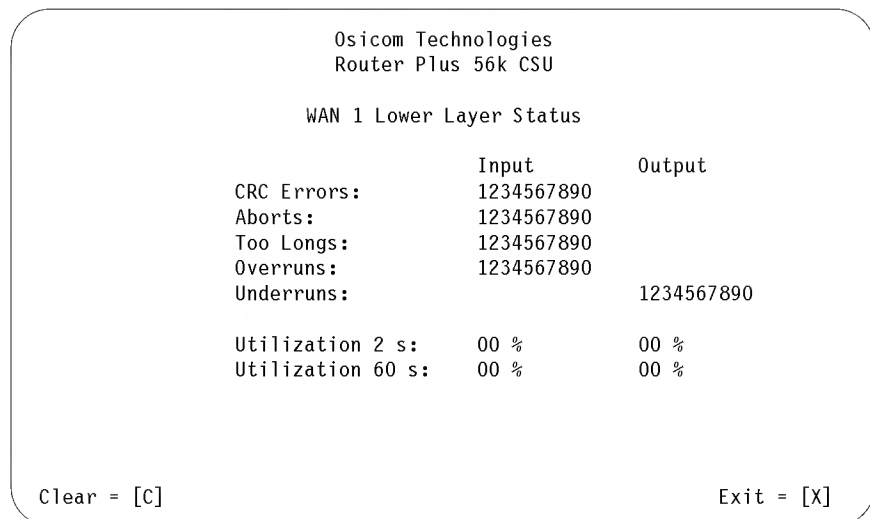
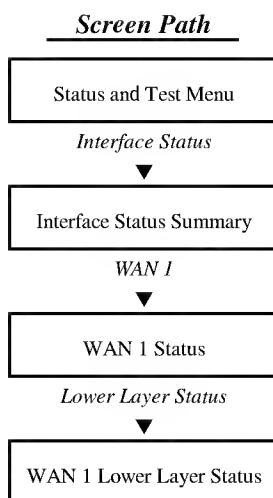


Figure 4-9. WAN Lower Layer Status

4.5.2.2 Annex D Status

Use this screen to view operational information for Frame Relay. This option is displayed only if the protocol on the WAN Configuration screen is set for FR – Annex D. Also access the **DLCI Status Table**. The screen is updated every two seconds.

The counters are based on Frame Relay MIB RFC 1315.

Error Type - the type of error that was last seen on this interface, as follows:

Unknown Error	DLCMI Proto Err
Receive Short	DLCMI Unknown IE
Receive Long	DLCMI Sequence Err
Illegal DLCI	DLCMI Unknown Rpt
Unknown DLCI	No Error Since Reset

DLCMI is Data Link Connection Management Interface

Error Time - the system time when the last error condition was detected.

Error Data - a hexadecimal string containing as much of the packet as possible for the last packet containing an error that was seen on the interface.

Status Messages - Status Enquiry (output) frames sent to the network provider (the Frame Relay switch) or Status Response (input) frames received from the network provider. A Status Enquiry is sent to the network provider at intervals defined by the **Polling Interval** WAN protocol parameter (default is 10 seconds).

Full Status Messages - Full Status Enquiry (output) frames sent to the network provider (the Frame Relay switch) or Full Status Response (input) frames received from the network provider. A Full Status Enquiry is sent to the network provider at intervals defined by the **Full Inquiry Interval** WAN protocol parameter (default is 6 seconds). The Full Status Response also contains information on the status of the Permanent Virtual Circuits (PVCs).

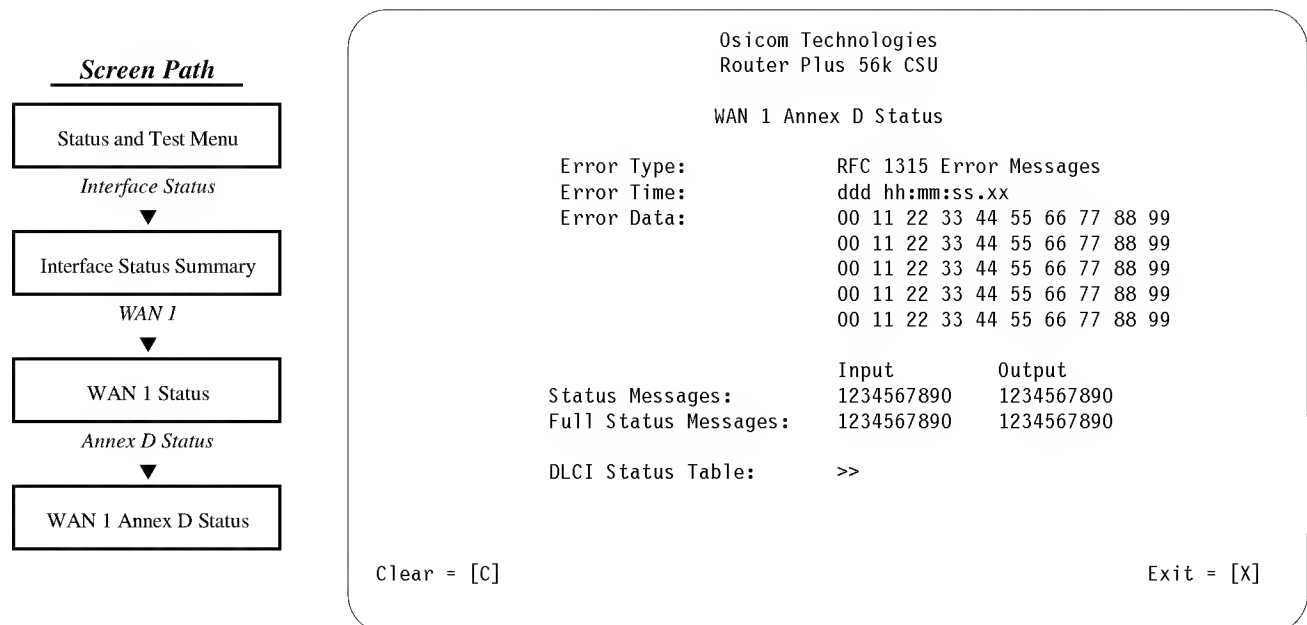


Figure 4-10. WAN Annex D Status (Frame Relay)

4.5.2.2.1 DLCI Status Table

Access the DLCI Status Table (Figure 4-11) to view the status of the DLCIs. (Fr - Annex D protocol only). This status is based on the LMI response received from the network (frame relay switch). This screen is updated every two seconds.

Page Down/Up prompts are displayed if there are more than 15 entries.

All DLCIs reported in LMI response are displayed.

DLCI - a Data Link Connection Identifier. The DLCI identifies the logical link on a Frame Relay network and is assigned by the network provider. Range is 0 to 1023.

State - the state of the DLCI as reported by the switch in response to the router's polls.

Active - the normal operating state; the DLCI is up.

Inactive - the DLCI is down.

Invalid - displayed if the switch reports a DLCI as active and the DLCI is configured on a port, but the DLCI **State** is set to disabled.

New - a newly-detected logical link.

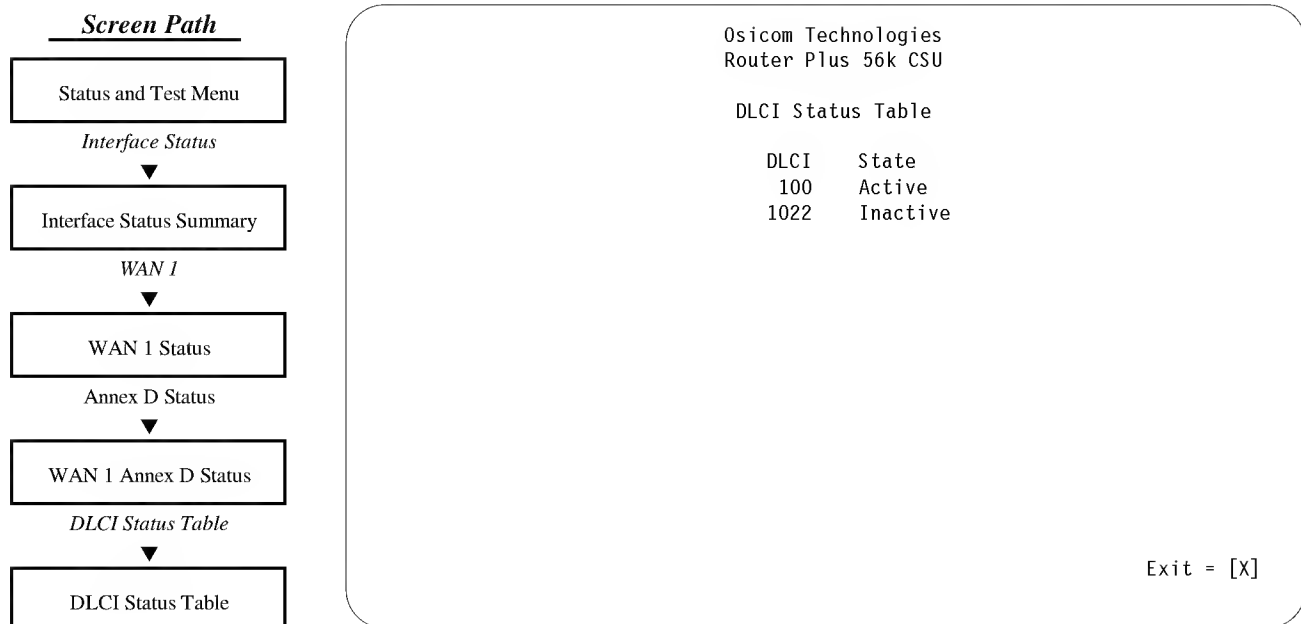


Figure 4-11. DLCI Status Table

4.5.3 WAN Status (PPP)

Figure 4-12 illustrates the WAN Status screen when PPP protocol is selected. The contents are identical to the WAN Status screen for Frame Relay except the Annex D Status selection is not available. This screen is updated every two seconds.

The counters are based on MIB II RFC 1213.

Press **[C]** to clear all counters.

Protocol - the configured protocol for the WAN interface.

Status - *Up* indicates the LCP is up.

Down indicates the LCP is down.

Octets - **Input**: all octets in each frame received from the SCC including the address and control fields but excluding the CRC. The value reported by the SCC includes the CRC. The CRC octets are subtracted before the counter is incremented. **Output**: all octets in each frame transmitted to the SCC including the address and control fields but excluding the CRC (the CRC is added by the SCC after it is received).

Unicast Packets - **Input**: all frames received from the SCC including LCP and NCP frames. **Output**: all frames transmitted to the SCC including LCP and NCP frames.

Discards - **Input**: the number of error free frames received by the SCC that the SCC could not forward because of no buffers. **Output**: the number of frames that the router or bridge could not forward because of no buffers.

Errors - **Input**: the total number of frames received in error. This includes any frames received with HDLC errors and format errors. HDLC errors (CRC, aborts, overruns, and too longs) are detected by the SCC and cause the appropriate error counter on the Lower Layer screen to increment. PPP format errors (bad address and bad control) are detected by software cause the appropriate error counter on the PPP Port Status screen to increment. Frames containing errors are not passed up to a higher layer protocol. **Output**: the total number of frames that an error occurred while transmitting. Output errors are detected by the SCC and also cause the Underrun counter on the Lower Layer screen to increment.

Unknown Protocol - **Input only**: the total number of frames received with the PPP protocol field set to a protocol that is not supported or is not enabled. Supported PPP protocol field values are LCP, IPCP, IPXCP, and BCP. Frames containing unknown protocols are not passed up to a higher layer protocol.

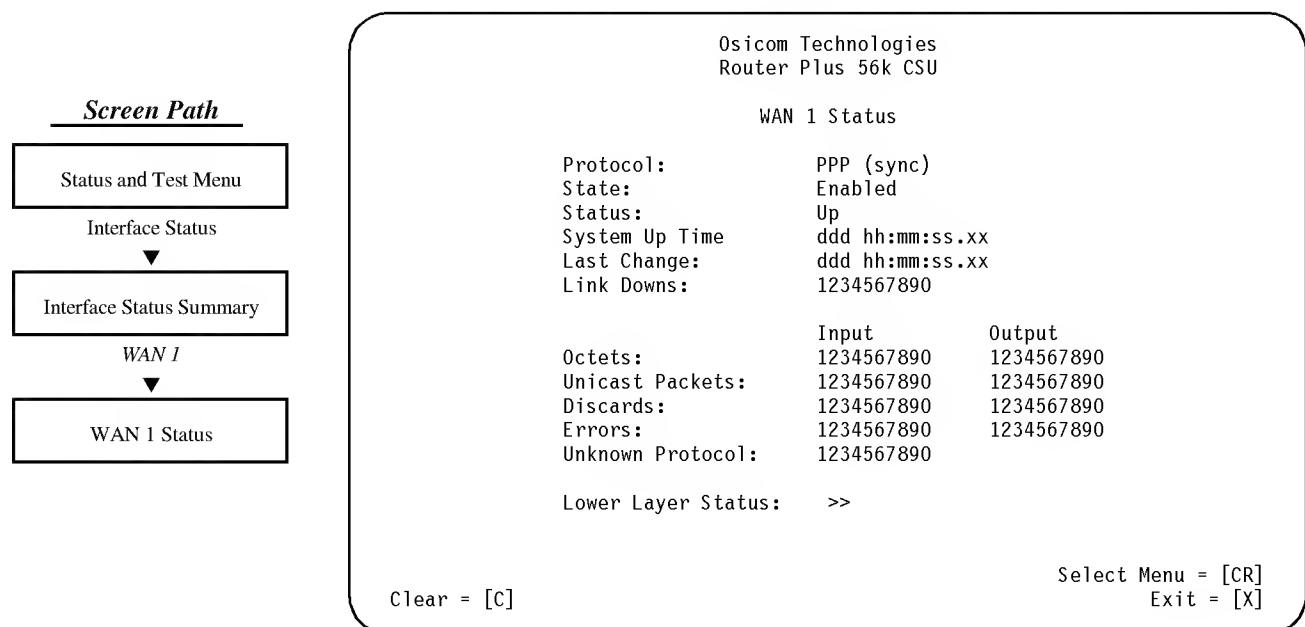


Figure 4-12. WAN Status (PPP)

4.6 Port Status Summary

The Port Status Summary screen (Figure 4-13) displays the operational status of ports configured on the router. You can view the status of up to 15 logical ports defined. Port 0 is always the LAN interface and ports 1 through 14 are always available for the WAN interface. This screen is updated every two seconds.

The table below defines port status for Frame Relay.

To view the status of a specific port, position the cursor on the port number and press **[CR]**; the port-specific screen is displayed. See Sections 4.6.1, 4.6.2, and 4.6.3.

The contents of the port-specific status screen depends on two factors:

- LAN or WAN interface
- Protocol selected

Port - number of the port (0 through 14).

Port Name - a name to identify this port when configuring and managing the router.

Interface - identifies the interface (LAN or WAN 1) to which the port is mapped. Port 0 is fixed at LAN.

Protocol - the configured LAN or WAN 1 connect protocol. For Frame Relay, the protocol field also displays the DLCI number and DLCI status.

Port Status (Frame Relay)		
PROTOCOL	STATUS	CONDITION
Fr-No LMI	Up/Down Disabled	Follows Interface Status DLCI state set to disabled *
FR-Annex D	Up Down Disabled	DLCI LMI status up DLCI LMI status down DLCI state set to disabled *
* See Port Status screen.		

NOTE

Only ports configured are shown.

Screen Path

Status and Test Menu

Port Status

▼

Port Status Summary

Osicom Technologies
Router Plus 56k CSU

Port Status Summary

Port	Port Name	Interface	Protocol
0	Local Site	LAN	Ethernet
1	Remote Site 1	WAN 1	FR-1000 Up
2	Remote Site 2	WAN 1	FR-1001 Down
3	Remote Site 3	WAN 1	FR-1002 Disabled

Cursor Down = [Space Bar]
 Cursor Up = [Backspace]

Select Menu = [CR]
 Exit = [X]

Figure 4-13. Port Status Summary

4.6.1 Port Status (LAN - Ethernet)

Figure 4-14 illustrates the Port Status screen for port 0, which is always the LAN interface. The protocol is fixed at Ethernet. This screen is updated every two seconds.

When any of the **Input** error counters increment, the **Input** error counters on the Interface Status screen also increment.

Incrementing any of the input error counters also causes the Input Errors counters to increment on the Interface Status screen. Incrementing the Excessive Collisions, Internal MAC Transmit Errors, or Carrier Sense Errors output error counters also causes the Output Errors counters to increment on the Interface Status screen.

See the Port Status Summary screen, page 18, for screen entries not defined here.

The counters are based on MIB RFC 1643.

Alignment Errors - received frames that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) test.

FCS Errors - received frames that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) test.

Frame Too Longs - received frames that exceed the maximum permitted frame size.

Internal MAC Receive Errors - received frames discarded due to an internal MAC sublayer receive error (Out of Buffers, Overruns).

Single Collision Frames - successfully transmitted frames on this interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - successfully transmitted frames for which transmission is inhibited by more than one collision.

Deferred Transmissions - number of frames for which the first transmission attempt is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.

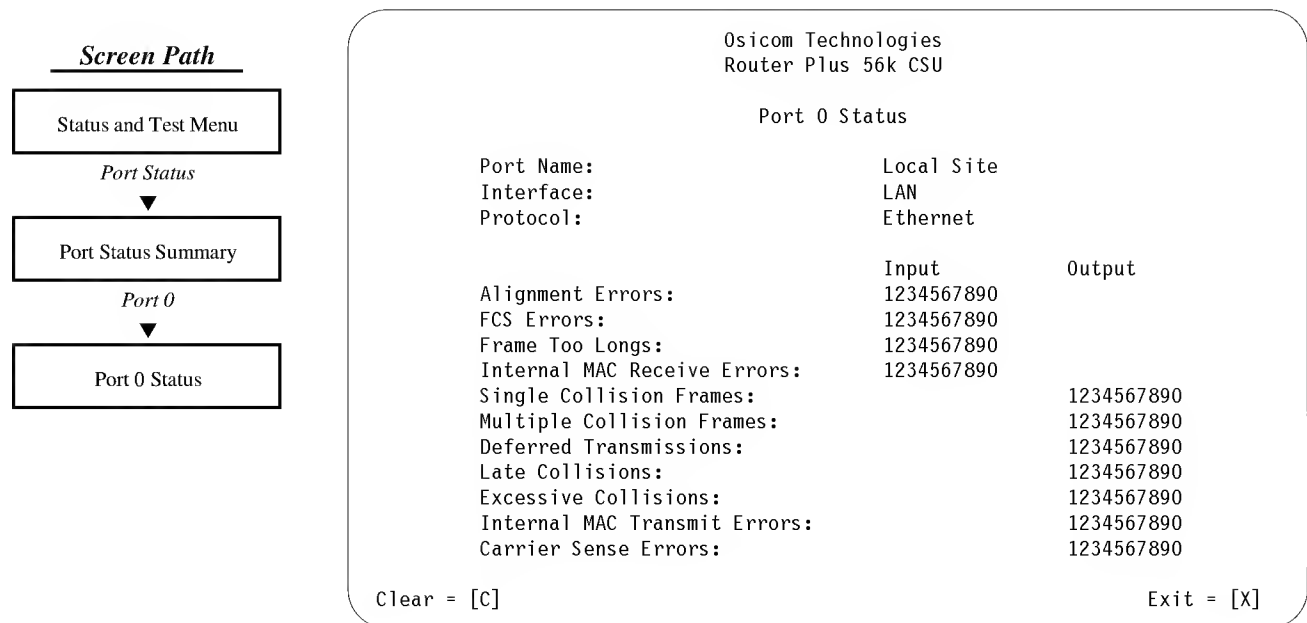


Figure 4-14. Port Status (LAN)

Late Collisions - number of times that a collision is detected on this interface later than 512 bit-times into the transmission of a frame. 512 bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.

Excessive Collisions - number of frames for which transmission fails due to excessive collisions. Retry limit is exceeded.

Internal MAC Transmit Errors - number of frames for which transmission fails due to an internal MAC sublayer transmit error.

Carrier Sense Errors - number of times that the carrier was not sensed (Carrier Lost, Tx Underrun, Tx Heartbeat) when attempting to transmit a frame on this interface. The count is incremented at most once per transmission attempt, even if the carrier fluctuates during a transmission attempt.

4.6.2 Port Status (WAN, Frame Relay)

Figure 4-15 illustrates a Port Status screen for a port on the WAN interface. The protocol selected is Frame Relay. This screen is updated every two seconds.

See the Port Status Summary screen, page 4-18, for screen entries not defined here.

The counters are based on MIB RFC 1315.

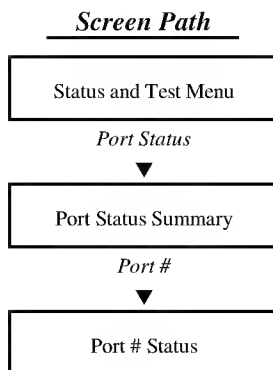
DLCI - the Frame Relay Data Link Connection Identifier configured for the specified port. The DLCI identifies the logical link on a Frame Relay network and is assigned by the network provider.

DLCI State - the configured status of the DLCI.

DLCI Status - the operational status of the DLCI.

System Up Time - the amount of time the unit has been operational (days:hours:minutes:seconds).

Creation Time - the system time when DLCI was established (days:hours:minutes:seconds). If protocol is FR - No LMI, this is the first time the DLCI came up after being defined.



Osicom Technologies
Router Plus 56k CSU

12:00:00

Port 1 Status

Port Name:	Remote Site 1	
Interface:	WAN 1	
Protocol:	FR - Annex D	
DLCI:	0025	
DLCI State:	Enabled	
DLCI Status:	Up	
System Up Time:	ddd hh:mm:ss.xx	
Creation Time:	ddd hh:mm:ss.xx	
Last Change:	ddd hh:mm:ss.xx	
Link Downs:	1234567890	

	Input	Output
FECNs:	1234567890	
BECNs:	1234567890	
Frames:	1234567890	1234567890
Octets:	1234567890	1234567890
Encrypted Frames:	0000000000	0000000000

Clear = [C]
Exit = [X]

Figure 4-15. Port Status (Frame Relay)

Last Change - the system time when the DLCI was most recently changed.

Link Downs - the number of times the DLCI has entered the link down state. This is mapped to the interface link downs counter for Frame Relay No LMI.

FECN - frames with the Forward Explicit Congestion Notification bit set. This bit is set when congestion (excess traffic) occurs between the router and the network.

BECN - frames with the Backward Explicit Congestion Notification bit set. This bit is set when congestion (excess traffic) occurs within the network.

Frames - all valid frames for this DLCI. This includes known protocol routed frames and bridged frames.

Octets - all octets (bytes) in each frame, including the DLCI, control field, and RFC 1490 encapsulation, but excluding the CRC.

Encrypted Frames - number of encrypted frames on this port (only displayed if encryption hardware is present).

4.6.3 Port Status (WAN, PPP)

Figure 4-16 illustrates a Port Status screen for a port on the WAN interface. The protocol selected is PPP. This screen is updated every two seconds.

Also view the **LCP** (Link Control Protocol), **IPCP** (IP Control Protocol), **IPXCP** (IPX Control Protocol), and **BCP** (Bridging Control Protocol) status screens.

When any of these error counters increment, the **Errors** counters on the WAN Interface Status screen also increment.

Encrypted Frames and the real time system clock are displayed only if encryption daughter card is present.

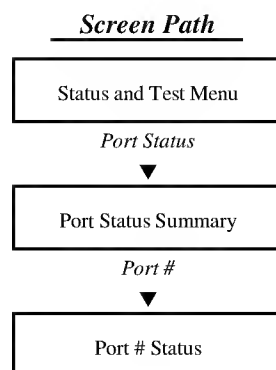
See the Port Status Summary screen, page 4-18, for screen entries not defined here.

The counters are based on MIB RFC 1471.

Bad Addresses - LCP or NCP (Network Control Protocol) frames received with an incorrect Address Field. The address field should have a value of FF.

Bad Controls - LCP or NCP frames received with an incorrect Control Field. The control field should have a value of 03.

See page 4-23 for an explanation of the status conditions.



Osicom Technologies
Router Plus 56k CSU
12:00:00

Port 1 Status

Port Name:	Port 1	
Interface:	WAN 1	
Protocol:	PPP (sync)	
	Input	Output
Bad Addresses:	0000000000	
Bad Controls:	0000000000	
Encrypted Frames:	0000000000	0000000000
LCP Status:	>> Closed	
IPCP Status:	>> Closed	
IPXCP Status:	>> Closed	
BCP Status:	>> Closed	

Cursor Down = [Space Bar]
Cursor Up = [Backspace]
Clear = [C]
Select Menu = [CR]
Exit = [X]

Figure 4-16. Port Status (PPP)

4.6.3.1 LCP Status

Access the Port LCP Status screen (Figure 4-17) to view the status of the Link Control Protocol (LCP) on ports with Point-to-Point Protocol selected. This screen is updated every two seconds.

The counters on the LCP Status screen are based on RFC 1661. LCP allows negotiation of certain characteristics of a point-to-point link. When a configuration option is not included in a *Configure Request* packet, the default value for that option is assumed.

Three classes of LCP packets that configure, terminate, and maintain a link are described below.

ESTABLISH AND CONFIGURE A LINK

The following link configuration packets are used to establish and configure a link:

Configure Requests - packets sent to open a connection. If a configuration option is not included in the packet, the default value for that configuration option is assumed.

Configure Acks - responses to Configure Request indicating all values are recognizable and acceptable.

Configure Nacks - responses to Configure Requests indicating all values are recognizable, but some are not acceptable.

Configure Rejects - responses to Configure Requests indicating some values are not recognizable or acceptable.

TERMINATE A LINK

The following link termination packets are used to terminate a link:

Terminate Requests - packets sent to close a connection.

Terminate Acks - responses to *Terminate Requests*.

MANAGE AND DEBUG A LINK

The following link maintenance packets are used to manage and debug a link:

Code Rejects - LCP packets with an unknown code.

Protocol Rejects - PPP packets with an unknown or unsupported protocol.

Discard Requests - packets which provide a Data Link Layer sink mechanism used for debugging and performance testing.

Echo Requests - packets which provide a mechanism used to determine if the remote unit is operational.

Echo Replies - messages sent in response to Echo Requests.

LCP State - the state of Link Control Protocol (based on RFC 1661).

Initial - the lower layer is unavailable (Down), and no Open has occurred. The Restart timer is not running.

Starting - the Open counterpart to the Initial state. An administrative Open has been initiated, but the lower layer is still unavailable (Down).

Closed - the link is available (Up), but no Open has occurred.

Stopped - the Open counterpart to the Closed state. It is entered when the system is waiting for a Down event or after sending a Terminate-Ack.

Closing - an attempt made to terminate the connection. A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received.

Stopping - the Open counterpart to the Closing state. A Terminate-Request has been sent and the Restart timer is running, but a Terminate-Ack has not yet been received.

Request Sent - an attempt made to configure the connection. A Configure-Request has been sent and the Restart timer is running, but a Configure-Ack has not yet been received.

Ack-Received - a Configure-Request has been sent and a Configure-Ack has been received. The Restart timer is still running, since a Configure-Ack has not yet been sent.

Ack-Sent - a Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. The Restart timer is running, since a Configure-Ack has not yet been received.

Opened - a Configure-Ack has been both sent and received.

Illegal - an event has occurred which has an internal error.

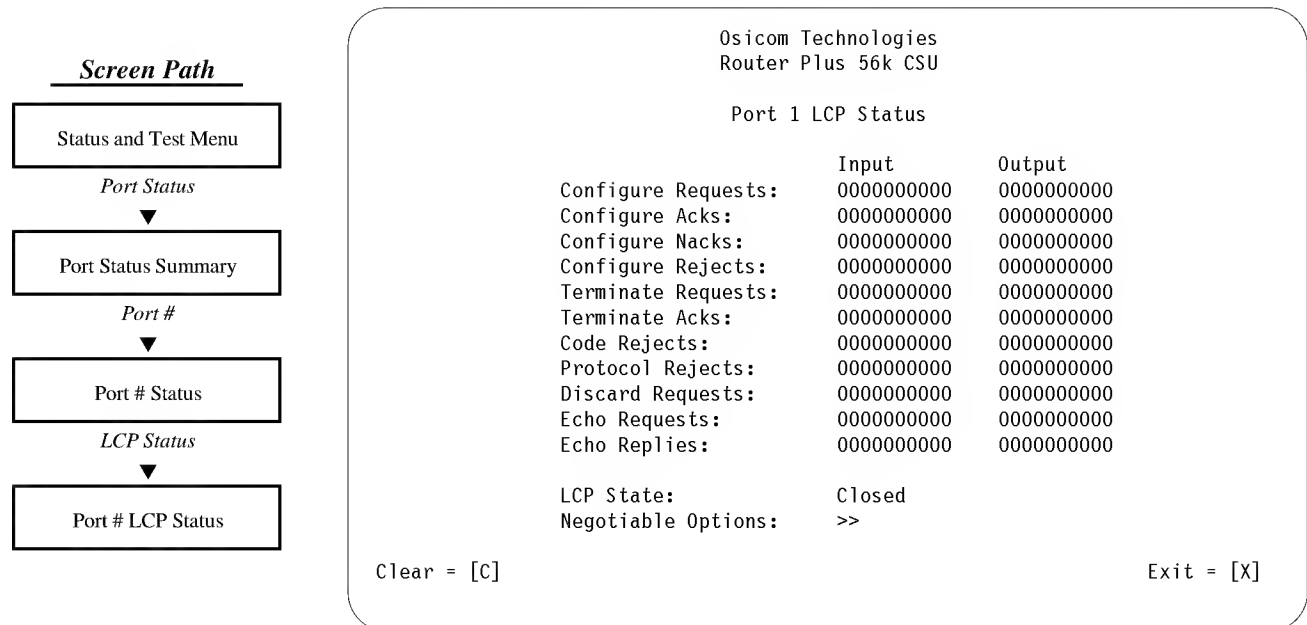


Figure 4-17. Port LCP Status (PPP)

4.6.3.1.1 LCP Negotiable Options

Access the LCP Negotiable Options screen (Figure 4-18) to view the values of LCP negotiable options in configuration requests sent and received by the router.

Negotiable options are based on RFCs 1661 and 1570.

Negotiable option status is determined after negotiation has been completed and Interface Status is up.

The **Local** field displays the option values in the last configuration request sent by the router.

The **Remote** field displays the option values in the last configuration request received by the router.

Maximum Receive Unit - specifies the maximum number of octets in the Information and Padding fields. It does not include the framing, Protocol field, FCS, nor any transparency bits or bytes. It is currently fixed at 1526.

Protocol Field Compression - provides a method to negotiate the compression of the PPP Protocol field. By default, all implementations must transmit packets with two-octet PPP Protocol fields.

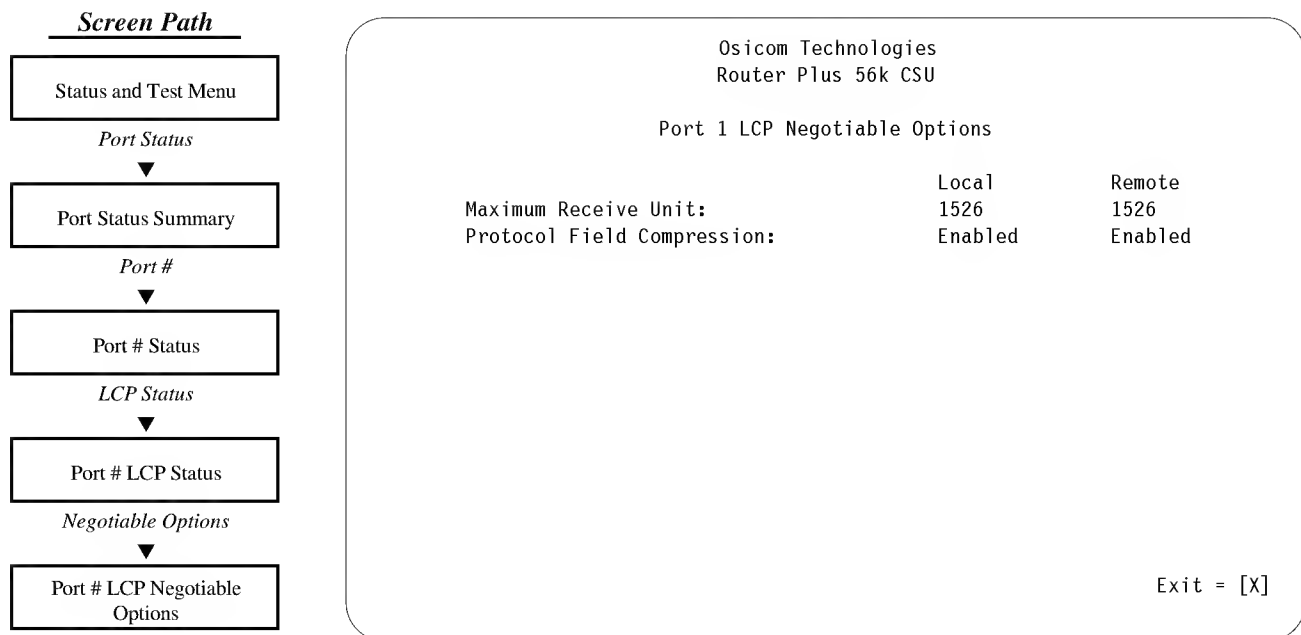


Figure 4-18. Port LCP Negotiable Options

4.6.3.2 IPCP Status

IP Control Protocol (IPCP) is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of a point-to-point link.

IPCP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPCP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPCP packets received before this phase is reached are discarded.

The router sends the configured IP Address in the IPCP configure requests.

If the remote peer rejects it, the router will stop insisting on it and remove the IP Address from the configure requests.

The router does not attempt to assign an IP address to its peer and does not request or accept an IP address from its peer. In no event will the router force the remote to use the IP Address configured for its PPP port. That is, the router won't NAK the IP Address specified by the remote.

If the two addresses do not match, then the link will work, IPCP will open, but IP may not route properly. If the remote peer NAKs the IP Address, then it is stating that it wants the router to use the address it is specifying. In this case, the router will remove the IP Address from its IPCP configure requests but will not use the IP Address in the Peer's configure requests.

See LCP Status (Section 4.6.3.1, page 4-22) for descriptions of counters.

See page 4-23 for an explanation of the various **State** conditions.

This screen is updated every two seconds.

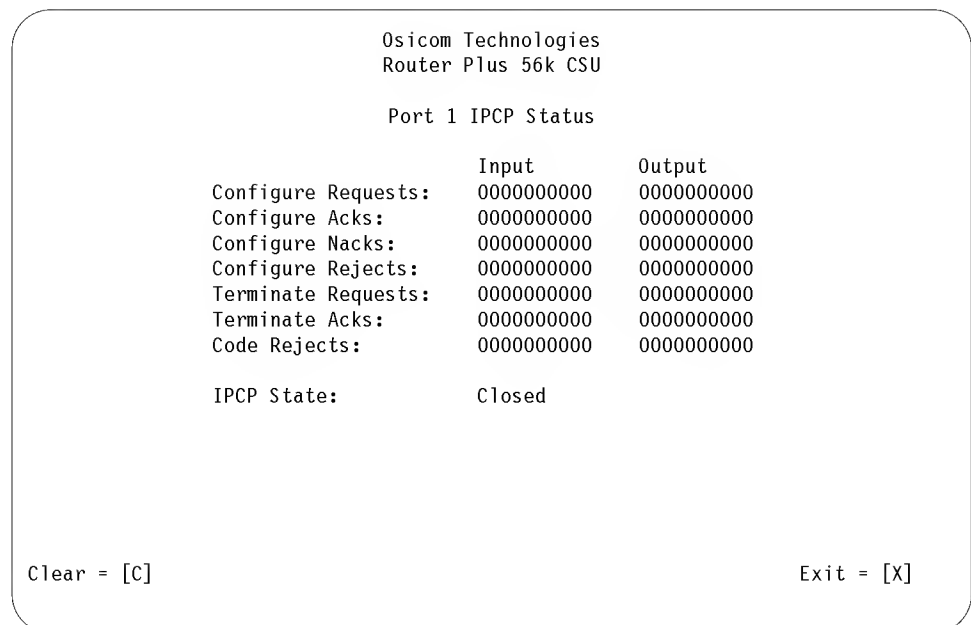
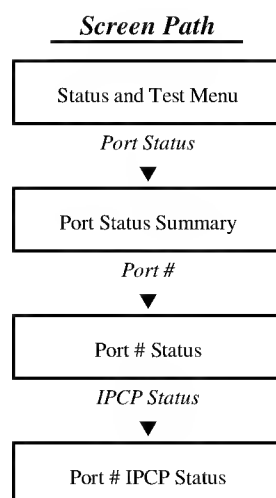


Figure 4-19. Port IPCP Status (PPP)

4.6.3.3 IPXCP Status

Figure 4-20 illustrates the IPXCP Status screen. IPX Control Protocol (IPXCP) is responsible for configuring, enabling, and disabling the IPX protocol modules on both ends of the point-to-point link.

IPXCP uses the same packet exchange mechanism as the Link Control Protocol. IPXCP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPXCP packets received before this phase is reached are discarded.

IPXCP Configuration Options allow modifications to the standard characteristics of the network-layer protocol to be negotiated. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

See LCP Status (Section 4.6.3.1, page 4-22) for descriptions of counters.

See page 4-23 for an explanation of the various **State** conditions.

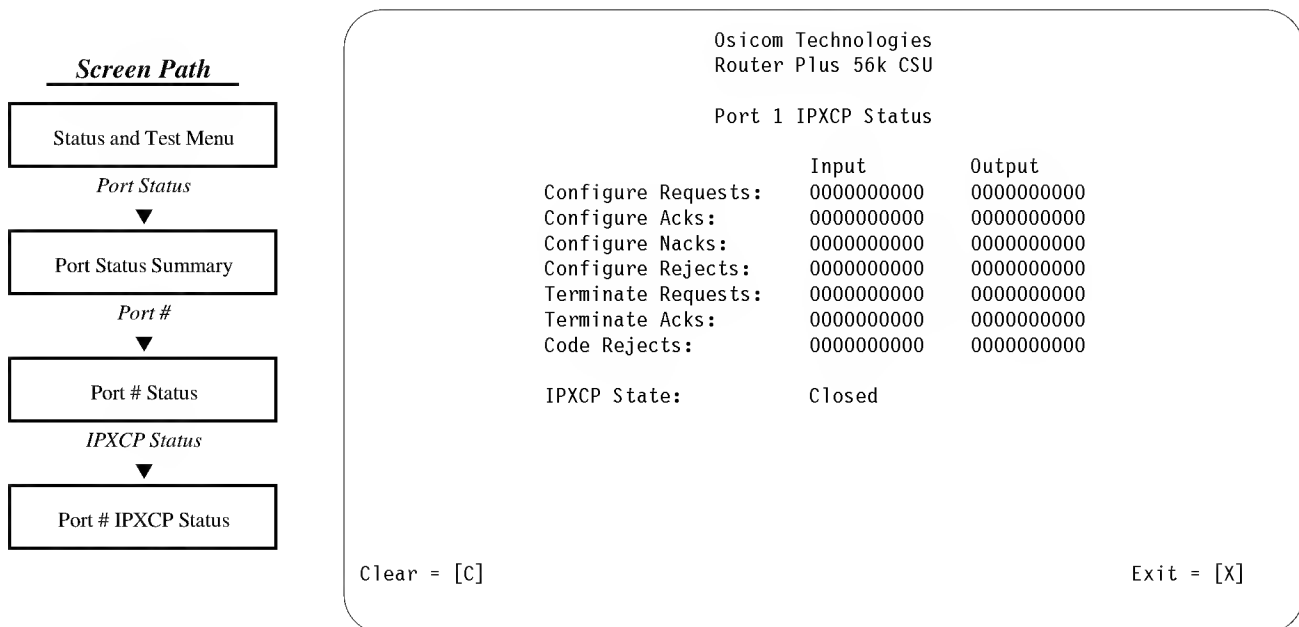


Figure 4-20. Port IPXCP Status (PPP)

4.6.3.4 BCP Status

The Bridging Control Protocol (BCP) is responsible for configuring, enabling and disabling the bridge protocol modules on both ends of the point-to-point link.

BCP uses the same packet exchange mechanism as the Link Control Protocol. BCP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. BCP packets received before this phase is reached are discarded.

See LCP Status (Section 4.6.3.1, page 4-22) for descriptions of counters.

See page 4-23 for an explanation of the various **State** conditions.

This screen is updated every two seconds.

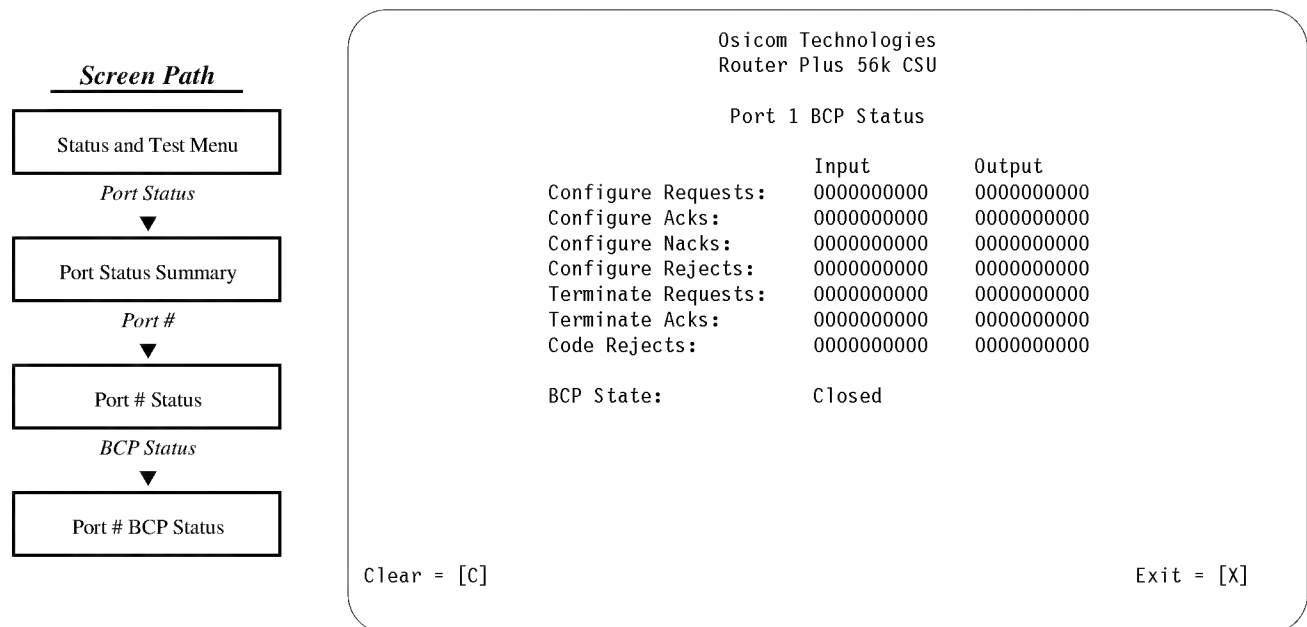


Figure 4-21. Port BCP Status (PPP)

4.7 TCP/IP Status and Test Menu

The TCP/IP Status and Test menu (Figure 4-22) is the top-level screen from which the user selects:

- Ping/Trace Route
- IP Status
- ICMP Status
- TCP and UDP Status
- SNMP Status
- ARP Table

Select Ping/Trace Route to display the command line interface (see Figure 4-23).

4.7.1 Ping/Trace Route

Use the **ping** command to verify if a gateway (router) or host is reachable from your router.

Use the **tracert** command to record (trace) routes from your router to a specified host or gateway (router).

When you select **Ping/Trace Route** from the TCP/IP Status and Test Menu, the screen shown in Figure 4-23 appears.

Invalid Commands

If an invalid command is entered, the following message appears:

Command is invalid. Type 'exit' to exit.

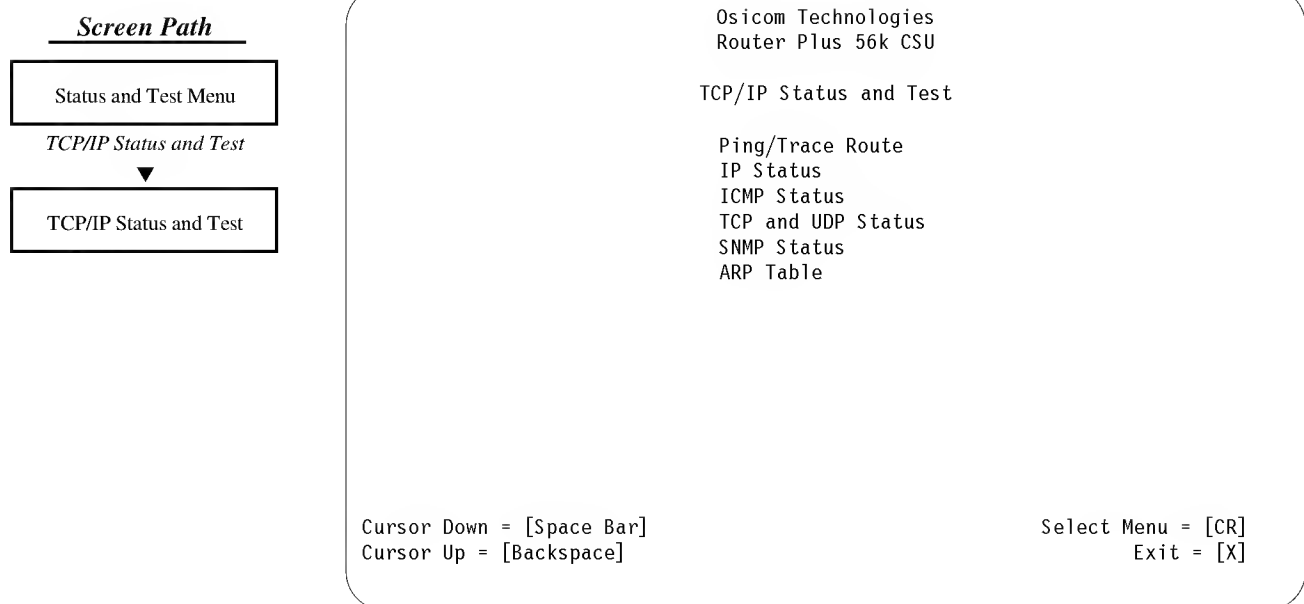


Figure 4-22. TCP/IP Status

Ping Command

The format for the ping command is:

```
ping <address>
```

where <address> is an IP address in either dotted decimal notation or hex notation (x7d00006d=125.0.0.109).

When the ping command is entered and a response is received, the following is displayed:

```
PING 125.0.0.109
125.0.0.109 is alive, RTT=5ms.
```

If no response is received within 5 seconds, the following message appears:

```
PING 125.1.2.3
Ping: No reply.
```

If the destination is unreachable (i.e., no route), the following message appears:

```
PING 1.2.3.4
Destination unreachable (1.2.3.4)
```

If you type ping without an address, the address from the last ping command will be used. If there is no previous ping in the current session, the invalid command message appears (see above).

Traceroute Command

The format for the traceroute command is:

```
traceroute <address>
```

where <address> is an IP address in either dotted decimal notation or hex notation (x7d00006d=125.0.0.109).

When you enter traceroute <address>, a UDP message is sent out to a bad port (33467). Packets are sent in groups of 3. The first group has its TTL set to 1. This causes the first router to send back a ICMP TTL EXCEEDED message. The source address of the ICMP message and how long it took for it to come back is recorded. This same message is sent two more times to get a set of three round-trip-times to the first router. Then, the second group of three UDP messages is sent with a TTL of 2. This causes the second router in the trace to send back ICMP TTL EXCEEDED messages. This continues until the reply that we receive is an ICMP PORT UNREACHABLE instead of a ICMP TTL EXCEEDED. This indicates that the final destination has been reached.

If a reply is not received within 5 seconds, the next packet is sent and a * is displayed in the time entry for the missed packet. Note the following examples.

A simple traceroute of a host on the same network as the Routermate Plus would show something like:

```
TRACEROUTE 125.0.0.109
1 125.0.0.109 4 ms 3 ms 4 ms
```

This indicates that the 3 packets in the group took 4, 3, and 4 ms. respectively.

For a host that is multiple hops away, an output may look like:

```
TRACEROUTE 131.143.16.1
1 125.0.0.75 3 ms 4 ms 3 ms
2 131.143.16.9 91 ms 91 ms 90 ms
3 131.143.16.1 95 ms 95 ms 95 ms
```

If the third packet from 131.143.16.1 had not been received, the last line of the output would look like:

```
3 131.143.16.1 95 ms 95 ms
0.0.0.0 * ms
```

It is possible that all three packets in a group may not be received from the same router. This can occur if a router goes down during the traceroute. In this case, an output like this may appear:

```
2 131.143.16.9 95 ms
131.143.16.8 98 ms 99 ms
```

This indicates that, for the second hop of the trace, a reply was received from 131.143.16.9 for the first packet in the group. The second and third packet replies came from 131.143.16.8.

Help

Enter help to re-display the command line interface.

Exit

Enter exit to return to the TCP/IP Status and Test Menu.

ROUTERmate Plus Command Line Interface

```
Usage:
ping (address)
traceroute (address)
help
exit
```

Commands>

Figure 4-23. Ping/Trace Route Screen

4.7.2 IP Status

The IP Status screen (Figure 4-24) displays information and statistics for the Internet Protocol (IP) for all ports on the router which are configured for IP routing. Also access the **IP Port Counters** screen. This screen is updated every two seconds.

The counters are based on MIB II RFC 1213.

INPUT DATAGRAMS

Received - input datagrams received, including those received in error.

Forwarded - datagrams forwarded.

Header Error - input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Address Error - input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at the local router. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported classes (e.g., Class E).

Unknown Protocol - locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Discarded - input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Delivered - input datagrams successfully delivered to IP user-protocols (including ICMP, UDP, BootP, and TCP).

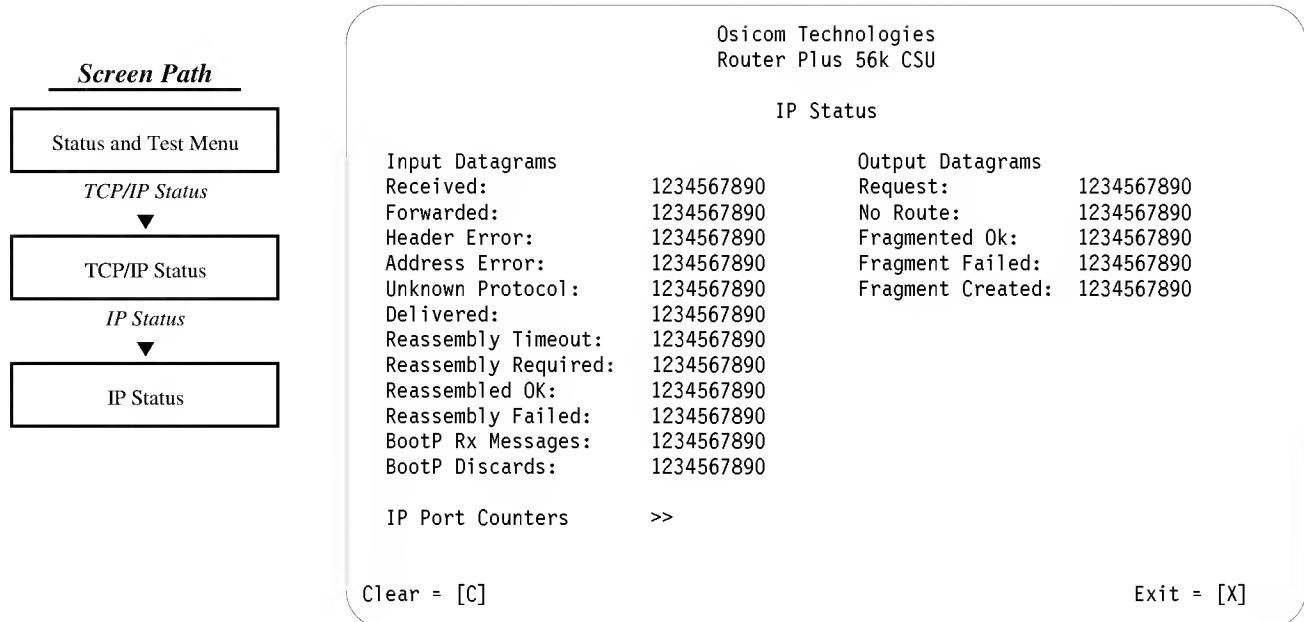


Figure 4-24. IP Status

Reassembly Timeout - the maximum number of seconds during which received fragments are held while they are awaiting reassembly.

Reassembly Required - IP fragments received that are waiting to be reassembled.

Reassembly Ok - fragmented IP datagrams received and successfully re-assembled.

Reassembly Failed - failures detected during the re-assembly of fragmented datagrams.

BootP Rx Messages - counter for received BootP Messages processed by the BootP Relay. This includes BootP requests from the client which are addressed to the BootP server UDP port. The BootP replies from the server are Routed to the Gateway router (the first router to receive the BootP request message from the Client) so the only router that counts BootP responses from the server is the Gateway Router.

BootP Tx Messages - counter for forwarded BootP messages processed by the BootP Relay. This includes BootP requests from the client which are addressed to the BootP server UDP port. The BootP replies from the server are Routed to the Gateway router (the first router to receive the BootP request message from the Client) so the only router that counts BootP responses from the server is the Gateway Router.

BootP Discards - counter for BootP messages discarded by the BootP Relay. This includes BootP messages discarded because of the BootP Threshold Seconds or BootP Threshold Hops options. It also counts BootP messages discarded because of errors.

OUTPUT DATAGRAMS

Request - IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in Input Datagrams Forwarded.

Discarded - output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). This counter includes datagrams counted in Input Datagrams Forwarded if any such packets met this discard criterion.

No Routes - IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in Input Datagrams Forwarded which meet this 'no-route' criterion. It also includes any datagrams not routed because the default route is down.

Fragmented Ok - IP datagrams that have been successfully fragmented for transmission.

Fragment Failed - IP datagrams that have been discarded because they needed to be fragmented but could not be (e.g., because their Don't Fragment flag was set).

Fragment Created - fragments that have been created from the fragmented datagrams.

4.7.2.1 IP Port Counters

Access the IP Port Counters screen (Figure 4-25) from the IP Status screen. Use this screen to view the number of datagrams received and transmitted on each port configured for IP routing.

This screen is updated every two seconds.

Address - the address configured for the port is displayed or *Unnumbered* is displayed if a WAN port is in Unnumbered mode.

Total IP Datagrams In - IP packets received on the specified port.

Total IP Datagrams Out - IP packets transmitted out the specified port.

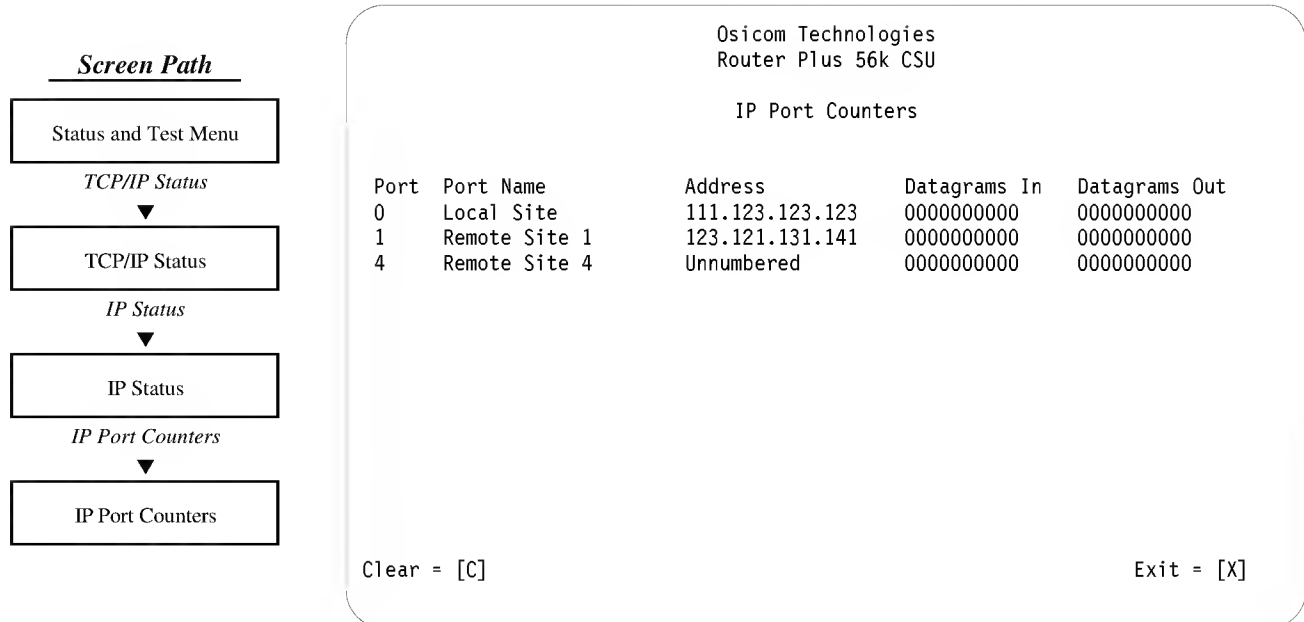


Figure 4-25. IP Port Counters

4.7.3 ICMP Status

The ICMP Status screen (Figure 4-26) displays information and statistics for the Internetwork Control Message Protocol (ICMP) for all ports on the router which are configured for IP routing. This screen is updated every two seconds.

ICMP allows gateways (routers) to send error or control messages to other gateways or hosts; ICMP provides communication between the IP software on one machine and the IP software on another.

The counters are based on MIB II RFC 1213.

Errored - ICMP messages with ICMP-specific errors (bad ICMP checksums, bad length).

Destination Unreachable - a message sent to the source indicating the datagram cannot be routed or delivered.

Time Exceeded - a message sent to the source when a datagram is discarded because its hop count has reached zero. Each IP datagram contains a time-to-live counter, called a *Hop Count*. To prevent datagrams from circling the Internet forever, each router/gateway decrements the count and discards the datagram when it reaches zero.

Parameter Problem - a message sent to the source indicating a problem with the datagram header. This message is only sent when the problem is so severe that the datagram must be discarded.

Source Quench - a message sent to the original source requesting that it slow down its rate of sending datagrams. When datagrams arrive too quickly for a gateway or router to process, the datagrams are discarded.

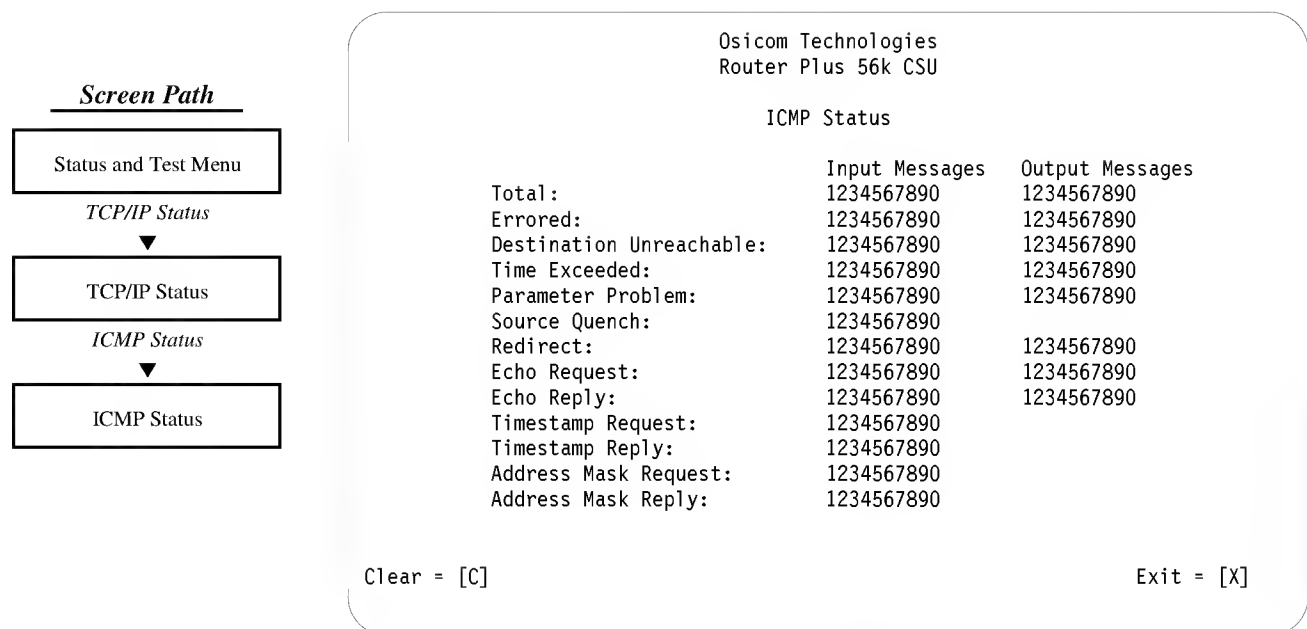


Figure 4-26. ICMP Status

Redirect - a message sent by a gateway to a router on a directly-connected network indicating a non-optimum route has been used.

Echo Request - a message sent to test whether a destination is alive and reachable (Ping Request).

Echo Reply - a message sent in response to an Echo Request (Ping Reply).

Timestamp Request - a message sent requesting the destination device return its current value for the time of day.

Timestamp Reply - a message returned to the device making a Timestamp Request.

Address Mask Request - a message sent to request the subnet mask of a device. The router does not send this message.

Address Mask Reply - a message returned to the device making an Address Mask Request.

4.7.4 TCP and UDP Status

The TCP and UDP Status screen (Figure 4-27) displays protocol information and statistics for all router ports that are configured for IP routing. Also access the **TCP Connection Table**. This screen is updated every two seconds.

The protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

The counters are based on MIB II RFC 1213.

TCP COUNTERS: (Transmission Control Protocol)

Retransmission Minimum - the minimum value permitted for the retransmission timeout value (milliseconds).

Retransmission Maximum - the maximum value permitted for the retransmission timeout value (milliseconds).

Maximum Connections - the limit on the total number of TCP connections supported.

Active Opens - TCP connections made by the router.

Passive Opens - TCP connections made to the router.

Attempt Fails - attempted TCP connections that failed, including both those attempted by the router and to the router.

Established Resets - resets received from established connections (a reset is made if the remote end is not connected).

Current Established - active TCP connections.

Input Segments - segments received, including those received in error. This count includes segments received on currently established connections.

Output Segments - segments sent, including those on current connections but excluding those containing only retransmitted octets.

Retransmitted Segments - segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

Received in Errors - segments received in error (e.g., bad TCP checksums).

Output RST Flags - resets sent from the router.

UDP COUNTERS: (User Datagram Protocol)

Input Datagrams - UDP datagrams received and delivered to UDP users.

No Ports - received UDP datagrams for which there was no known application at the destination port.

Input Errors - received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Output Datagrams - UDP datagrams sent from the local router.

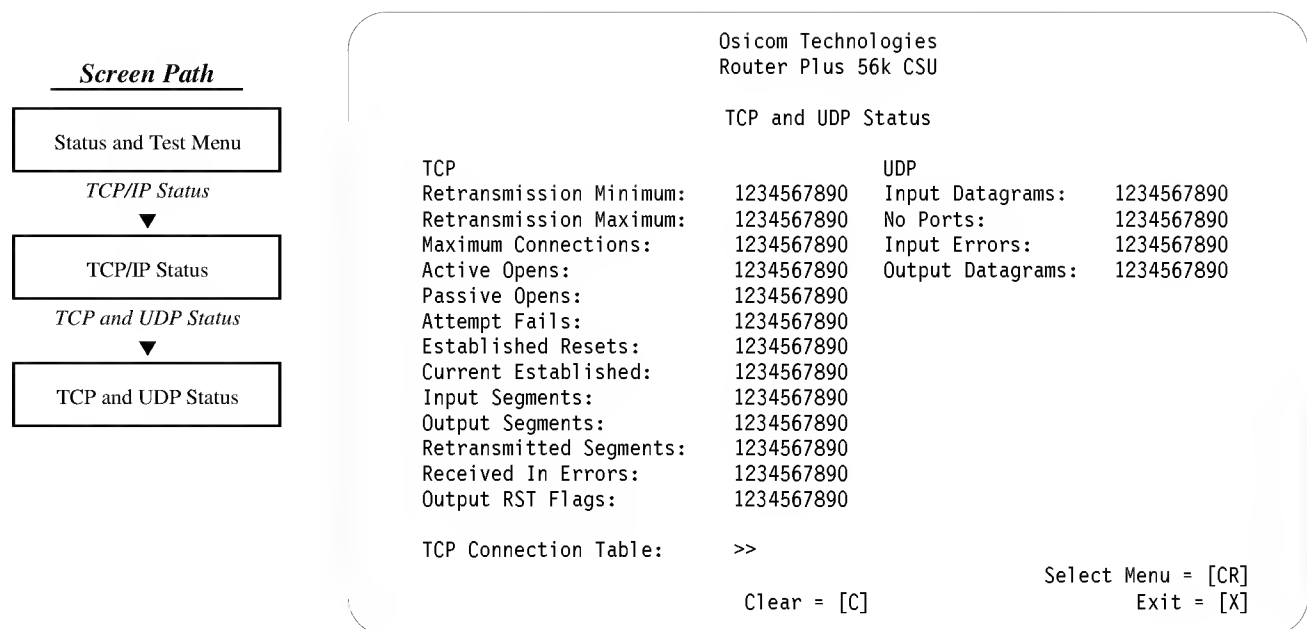


Figure 4-27. TCP and UDP Status

4.7.4.1 TCP Connection Table

Access the TCP (Transport Control Protocol) Connection Table (Figure 4-28) from the TCP and UDP Status screen. This screen displays MIB II information about the router's existing TCP connections.

This screen is updated every five seconds.

The counters are based on MIB II RFC 1213.

Connection State - status of this TCP connection.

Closed
Listen
SynSent
SynReceived
Established
FinWai56k
FinWait2
CloseWait
LastAck
Closing
TimeWait
Delete TCB (connection terminated)

Local Address - local IP address assigned to the link.
A connection in the listen state that is willing to accept connections for any port is set to 0.0.0.0.

Local Port - local port number for this TCP connection.

Remote Address - remote IP address for this TCP connection.

Remote Port - remote port number for this TCP connection.

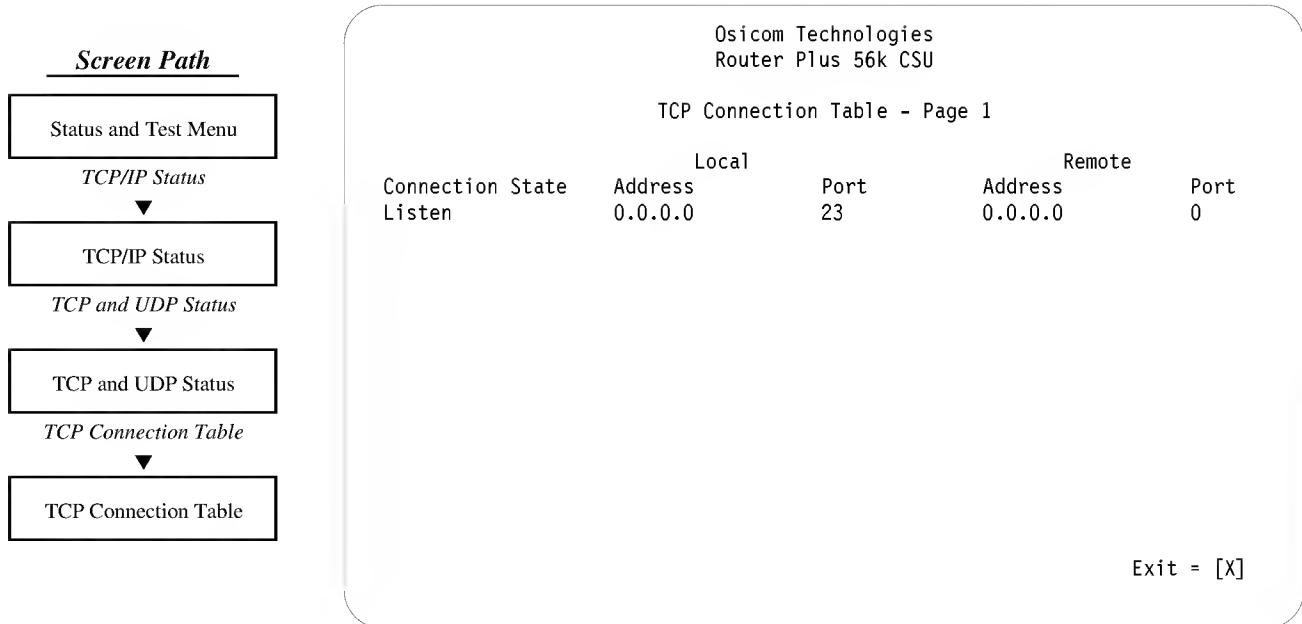


Figure 4-28. TCP Connection Table

4.7.5 SNMP Status

Use the SNMP Status screen (Figure 4-29) to view the status of SNMP (Simple Network Management Protocol) messages. This screen is updated every two seconds.

Press **[C]** to reset the counters to zero.

In the following descriptions, an SNMP Protocol Data Unit (PDU) is SNMP information that is encapsulated in a UDP datagram.

The counters are based on MIB II RFC 1213.

Packets - SNMP messages delivered between the local router and the transport service.

Bad Versions - SNMP messages which were delivered that were for an unsupported SNMP version.

Bad Community Names - SNMP messages delivered which used an unknown SNMP community name.

ASN Parse Errors - the total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.

Bad Community Uses - SNMP messages delivered that represented an SNMP operation which was not allowed by the SNMP community named in the message.

Too Bigs - SNMP PDUs for which the value of the error-status field is 'too big.'

No Such Names - SNMP PDUs for which the value of the error-status field is 'noSuchName.'

Bad Values - SNMP PDUs for which the value of the error-status field is 'badValue.'

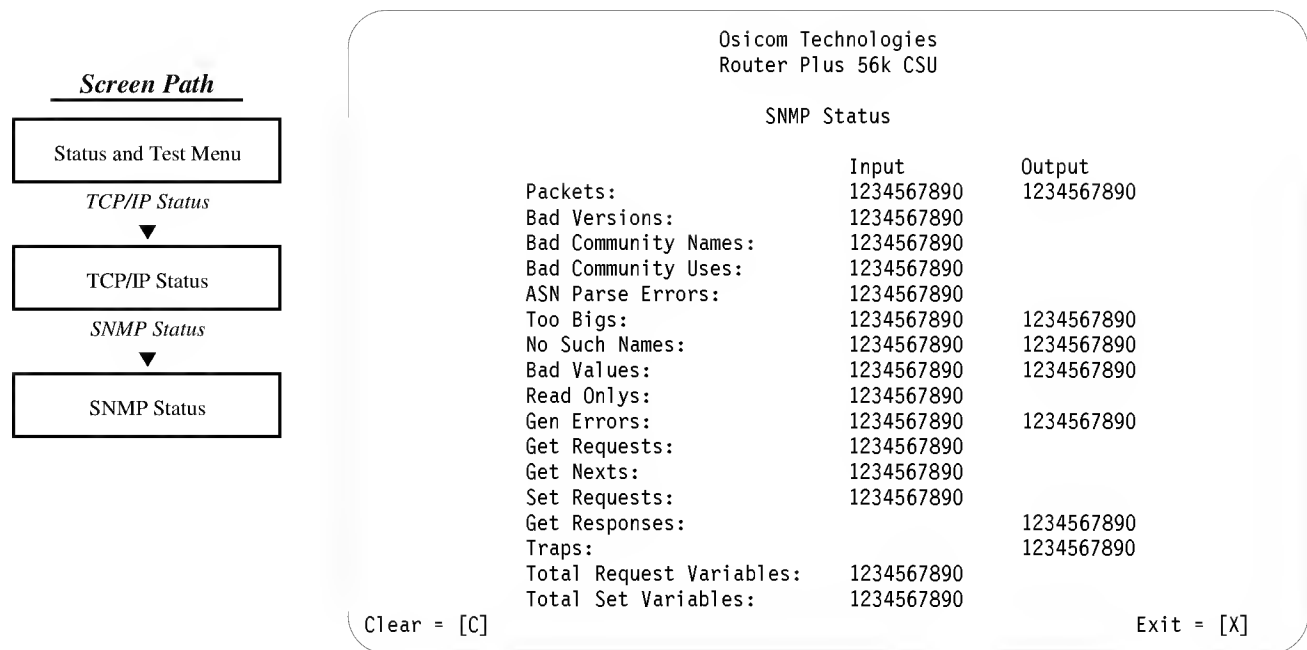


Figure 4-29. SNMP Status

Read Onlys - valid SNMP PDUs that were delivered for which the value of the error-status field is 'readOnly.' It is a protocol error to generate an SNMP PDU which contains the value 'readOnly' in the error-status field, as this object is provided as a means of detecting incorrect implementations of the SNMP Working Group.

Gen Errors - SNMP PDUs for which the value of the error-status field is 'genErr.'

Get Requests - SNMP Get-Request PDUs.

Get Nexts - SNMP Get-Next PDUs.

Set Requests - SNMP Set-Request PDUs.

Get Responses - SNMP Get-Response PDUs.

Traps - the number of traps sent.

Total Request Variables - MIB objects delivered successfully as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Total Set Variables - MIB objects which have been altered successfully as the result of valid SNMP Set-Request PDUs.

4.7.6 ARP Table

Access the ARP Table (Figure 4-30) to view IP addresses and corresponding MAC addresses for devices with which the router has communicated recently.

The router uses Address Resolution Protocol (ARP) to dynamically learn the MAC address of a destination router or host on the same physical network. A receiver updates its ARP table before processing an ARP packet. This screen is updated every five seconds.

Page Down/Page Up prompts appear when there are more than 15 entries in the table.

The counters are based on MIB II RFC 1213.

Press **[F]** to clear the table.

Physical Address (48-bit hex) - the physical Media Access Control (MAC) address.

Network Address - IP address corresponding to the physical MAC address.

Type - the address as one of the following:

Invalid - no response to an ARP request was received.

Dynamic - the IP address for this router was learned automatically from an ARP message.

Age - number of seconds since the last ARP packet was received.

- The ARP timer is incremented once a minute for Dynamic entries and once a second for Invalid entries.
- An Invalid entry is one that is waiting for an ARP reply.
- The timeout for Invalid entries is set at 2 seconds with 3 retries. Dynamic entries are maintained in the list for 60 minutes. If they are not updated within that limit, they are deleted.

Screen Path

Status and Test Menu

TCP/IP Status
▼

TCP/IP Status

ARP Table
▼

ARP Table

Osicom Technologies
Router Plus 56k CSU

ARP Table - Page 1

Physical Address	Network Address	Type	Age
08:00:20:0F:F5:ED	125.0.1.1	Dynamic	0060
08:00:20:0F:F5:E0	125.0.0.1	Dynamic	0060
08:00:20:0F:F5:E1	125.0.0.2	Dynamic	0060
08:00:20:0F:F5:E2	125.100.0.88	Dynamic	0120
08:00:20:0F:F5:E3	125.0.1.4	Dynamic	0180
08:00:20:0F:F5:E4	125.0.0.5	Dynamic	3480
08:00:20:0F:F5:E5	125.0.0.6	Dynamic	0120
08:00:20:0F:F5:E6	100.80.10.5	Dynamic	0009
08:00:20:0F:F5:E7	125.0.1.7	Dynamic	0060
08:00:20:0F:F5:E8	125.0.0.8	Dynamic	0120
08:00:20:0F:F5:E9	125.0.0.9	Dynamic	0180
08:00:20:0F:F5:02	125.125.125.125	Dynamic	0180
08:00:20:0F:F5:03	125.10.1.1	Dynamic	0060
08:00:20:0F:F5:04	125.1.1.1	Dynamic	0060
08:00:20:0F:F5:05	125.0.0.32	Dynamic	0060

Page Down = [+]
Flush = [F]
Exit = [X]

Figure 4-30. ARP Table

4.8 IPX Status

The IPX Status screen (Figure 4-31) is the top-level screen from which you can access and view the status of ports on which IPX routing is enabled. This screen is updated every two seconds.

NOTE

Only ports with IPX routing enabled are displayed.

To view the IPX status of a particular port, position the cursor on that port number and press **[CR]**.

Press **[C]** to clear all counters on the IPX, RIP/SAP, and IPXWAN screens.

Port - port number (0-14) for ports with IPX enabled.

Port Name - free-text description that is assigned at the Port Configuration screen for this port.

Address - 32-bit hexadecimal IPX network number that is assigned at the IPX Routing Options screen for this port, followed by the 48-bit hexadecimal value for the Node Number that is permanently assigned to the same value as the MAC address for the LAN interface.

Unnumbered is displayed if a WAN port is in unnumbered mode.

If IPXWAN is enabled, the network number may be a number assigned by IPXWAN instead of the number configured for the port. IPXWAN assigns the primary network number based on the master/slave relationship. If the local and remote router's WAN ports have different IPX network numbers, then the master unit will assign an IPX network number to the slave.

Packets In - total IPX packets received on the specified interface.

Packets Out - total IPX packets transmitted out the specified interface.

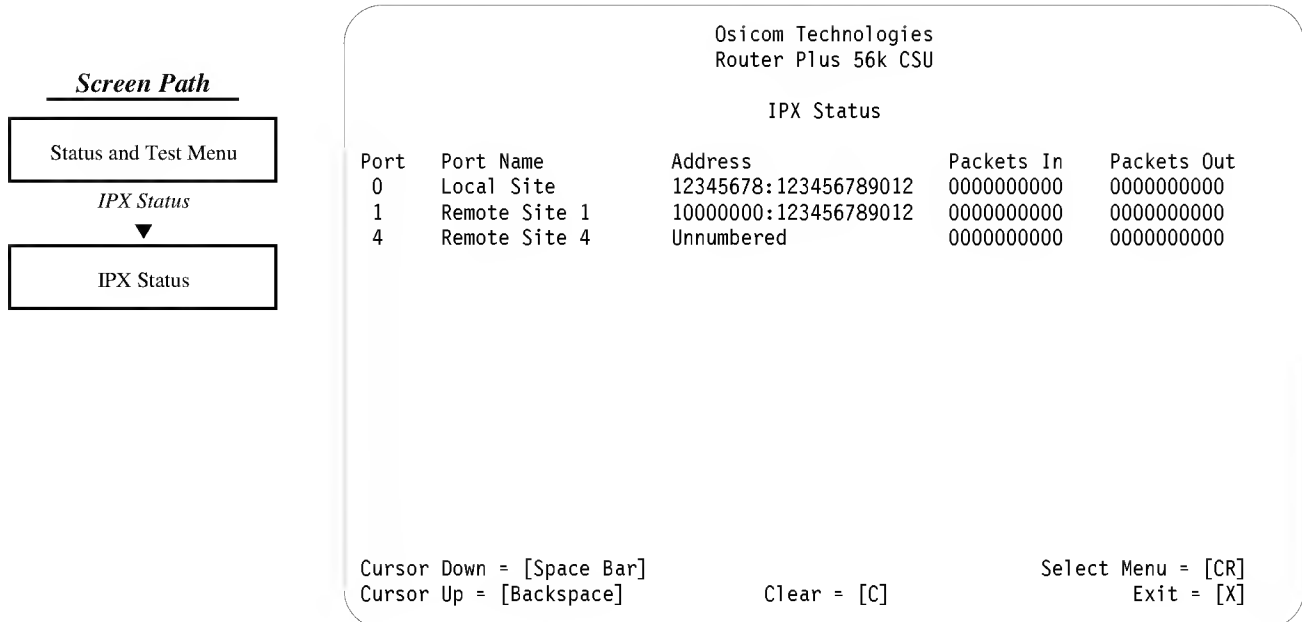


Figure 4-31. IPX Status

4.8.1 IPX Status (LAN and WAN)

The Port IPX Status screen (Figure 4-32, Port 0 and 4-33, Port 1) displays information and statistics for the Internetwork Packet eXchange Protocol (IPX) for ports on the LAN and WAN interfaces. This screen is updated every two seconds.

NOTE

The screens for LAN and WAN are identical except for the parameters indicated.

Two columns display various counters for received or transmitted frames, as follows:

- **Input** - applies to received IPX packets.
- **Output** - applies to transmitted IPX packets.

This screen also provides access to the **RIP/SAP Status** and **IPXWAN Status** screens (WAN only).

Total IPX Packets - IPX Packets on this port. This counter does not include Packets In error or Packets Too Long.

Packets To Route - total packets received that required routing.

No Route - packets received via the port that could not be forwarded because a path to the network is not known.

Hop Count Too Large - packets received on the port that were discarded because the transport control field (hop count) was greater than 14.

Packets In Error - packets with an invalid **Type** field or an incorrect packet length field.

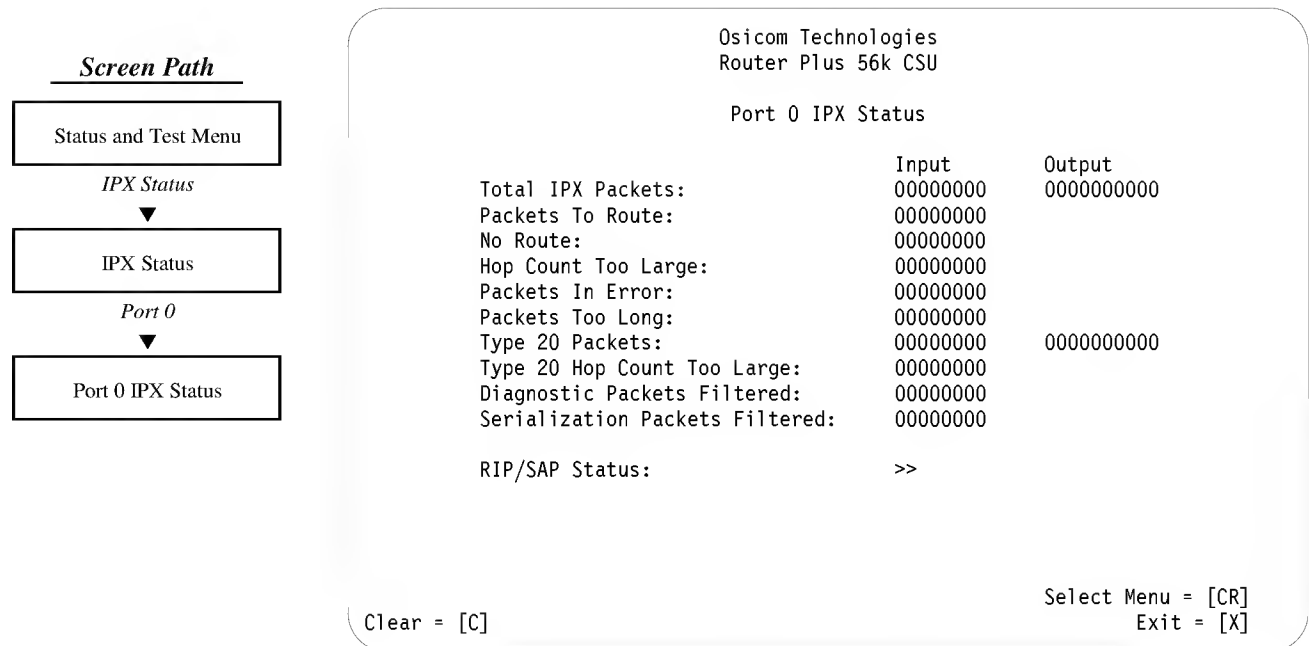


Figure 4-32. Port IPX Status (LAN)

Packets Too Long - packets received that were too long (based on the IPX header length field and the actual packet length).

Type 20 Packets - Novell encapsulated Netbios packets on the specified virtual IPX port.

Type 20 Hop Count Too Large - Netbios packets received on the port that were discarded because the hop count was too large. Type 20 packets received with a Transport Control field of 8 or greater are discarded.

Diagnostic Packets Filtered (LAN only) - diagnostic packets filtered due to the Diagnostic Packets option on the port IPX Filters screen.

Serialization Packets Filtered (LAN only) - serialization packets filtered due to the Serialization Packets option on the port IPX Filters screen.

Watchdog Requests Spoofed (WAN only) - the number of Watchdog Requests received on this port which were not forwarded due to watchdog spoofing. See the **Watchdog Packets** option on the port IPX Filters screen in Chapter 5.

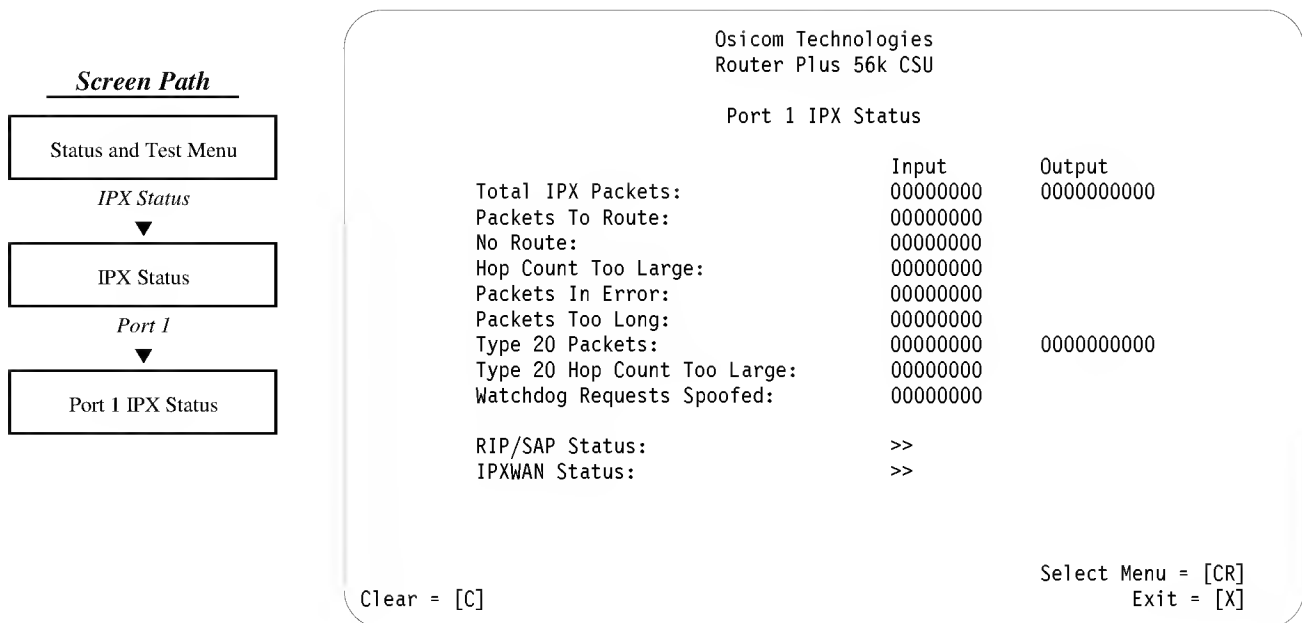


Figure 4-33. Port IPX Status (WAN)

4.8.1.1 IPX RIP/SAP Status (LAN and WAN)

The Port IPX RIP/SAP Status screen (Figure 4-34) displays statistics counters on SAP (Service Advertising Protocol) and RIP (Routing Information Protocol) packets for ports on the LAN and WAN interfaces. This screen is updated every two seconds.

SAP/RIP Responses Input: the total number of RIP/SAP responses received.

SAP/RIP Responses Output: the total number of solicited RIP/SAP responses (sent in response to a general and specific requests). This does not include unsolicited responses such as triggered updates or periodic updates.

SAP/RIP General Requests - general queries.

SAP/RIP Specific Requests - specific queries.

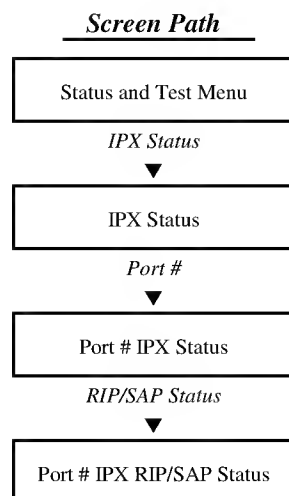
SAP/RIP Responses - general responses.

SAP Get Nearest Requests - nearest queries.

SAP Get Nearest Responses - nearest responses.

SAP/RIP Periodic Update - periodic router broadcasts.

SAP/RIP Triggered Update - update router broadcasts.



Osicom Technologies Router Plus 56k CSU		
Port 0 IPX RIP/SAP Status		
	Input	Output
SAP General Requests:	0000000000	0000000000
SAP Specific Requests:	0000000000	
SAP Responses:	0000000000	0000000000
SAP Get Nearest Requests:	0000000000	
SAP Get Nearest Responses:		0000000000
SAP Periodic Update:		0000000000
SAP Triggered Update:		0000000000
RIP General Requests:	0000000000	0000000000
RIP Specific Requests:	0000000000	
RIP Responses:	0000000000	0000000000
RIP Periodic Update:		0000000000
RIP Triggered Update:		0000000000
Clear = [C] Exit = [X]		

Figure 4-34. Port IPX RIP/SAP Status (LAN and WAN)

4.8.1.2 IPXWAN Status

IPXWAN is a protocol developed by Novell and specified in RFC1634. The purpose of IPXWAN is to provide a common way of exchanging router to router information across different type of wide area links. RFC1634 describes how Novell IPX operates over various WAN media using the IPXWAN protocol.

Support for IPXWAN is only provided to allow the router to be compatible with Novell routers. It is not required to route IPX and should be disabled unless it is required. The default is disabled.

NOTE

IPXWAN must be set to the same value on both ends of a connection. If it is not set to the same value, then the router will not be able to communicate across the link.

There are two steps in the IPXWAN operation:

1. Negotiate master/slave role.
2. Exchange router configuration information.

After these steps are concluded, transmission of IPX routing packets begins.

This screen is updated every two seconds.

Counter definitions are based on RFC 1634.

Timer Requests - a packet sent from both sides after link establishment which starts a timer and waits for a Timer Response. These packets are exchanged every 20 seconds until a response is received or a decision is made that the remote node is not responding.

Timer Responses - the reply to a Timer Request. This packet verifies each option in the Timer Request packet.

Information Requests - data packets sent (Master) after the peers have exchanged Timer Request and Response packets and negotiated options.

Information Responses - data packets received (Slave) after the peers have exchanged Timer Request and Response packets and negotiated options.

Nacks - received IPXWAN packets that were not acceptable. Either the received packet type was invalid or not recognized, or a badly-formed IPXWAN packet was received.

Bad Packets - illegal packets received.

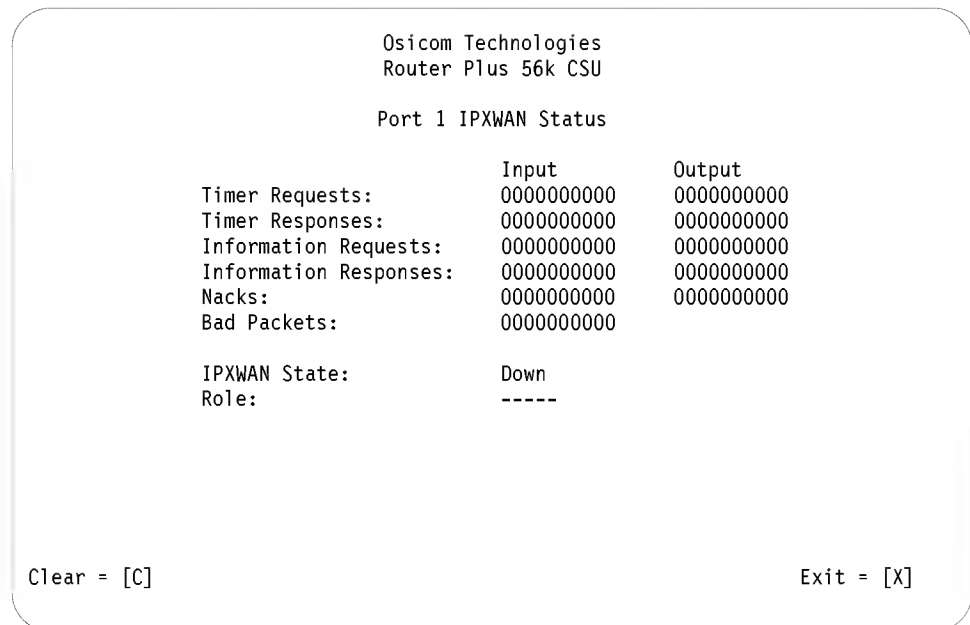
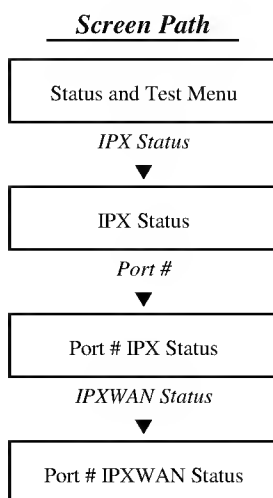


Figure 4-35. Port IPXWAN Status (WAN)

IPXWAN State - status of the negotiation.

Disabled: the IPXWAN option is disabled.

Down: negotiation failed.

Negotiating Timer: negotiating timer packets.

Negotiating Information: negotiating Information packets.

Up: negotiation complete.

Role - function of the local router. Upon receiving a Timer Request packet, the router determines its role for the remainder of the IPXWAN exchanges. This parameter is only used during IPXWAN initial negotiation to determine master/slave roles. The router with the higher Internal Network Number is the master.

Master: the requestor in the packet exchange.

Slave: the responder in the packet exchange.

Dashes (-----) displayed when the State is not *Up*.

Refer to RFC 1634 for details of these counters.

4.9 Bridging Status

Access the Bridging Status screen (Figure 4-36) to view a summary of received, discarded, and transmitted frames of ports on which bridging is enabled. This screen is updated every two seconds.

To display the status screen for any displayed port, move the cursor to the desired port and press **[CR]**.

Port - port number (0-14) for ports with bridging enabled.

Port Name - free-text description that is assigned at the Port Configuration screen for this port.

In Frames - total frames received.

Discards - total frames discarded.

Out Frames - total frames sent.

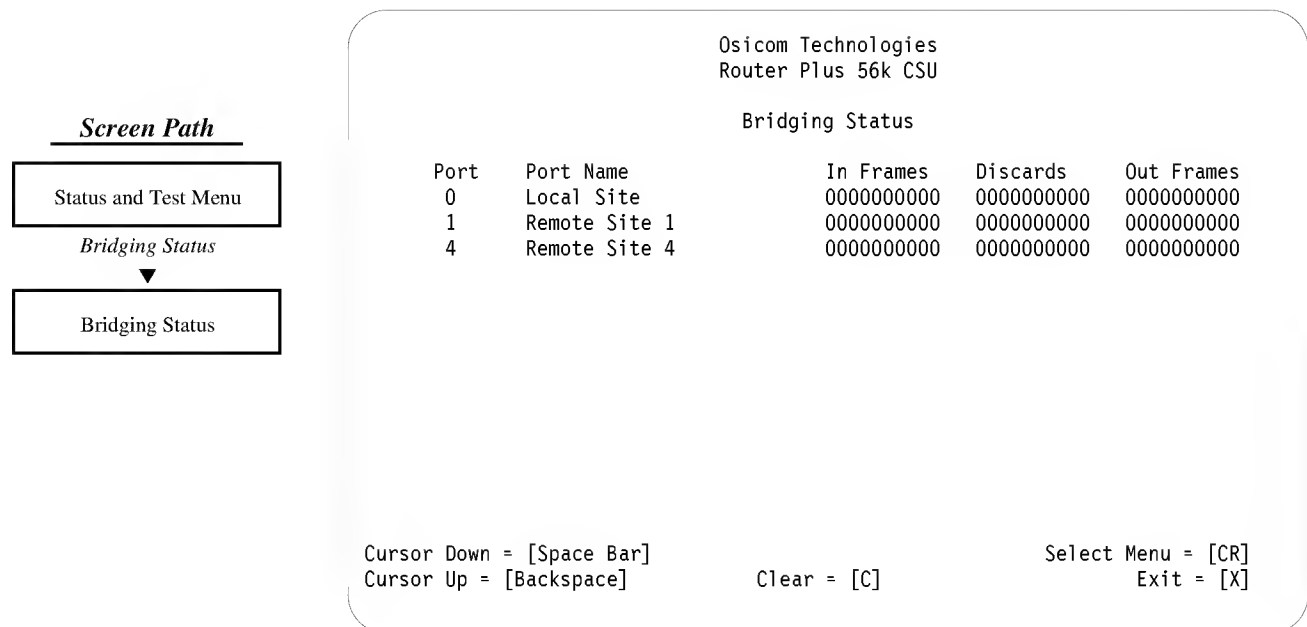


Figure 4-36. Bridging Status

4.9.1 Port Bridging Status

Access the Port Bridging Status screen (Figure 4-37) to display bridging status information for a specific port. This screen is updated every two seconds.

- Input - Received bridged frames.
- Output - Transmitted bridged frames.

Total Frames - frames sent/received on this port.

Too Shorts - frames on this port that were discarded because they were too short.

Normal Discards - frames on this port that were destined for the same port. This is normal.

Address Discards - frames discarded due to source or destination entries in the address table being marked as 'filter.'

Loop Discards - frames received from the wrong port. The port that the frame was received on was different than the port the source address was associated with in the Bridging Table.

Restricted Discards - frames discarded due to setting the forwarding mode to 'restricted.' If a frame is received by the bridge and its header does not contain the address of a device in the forwarding table, the frame is discarded and this counter is incremented.

Flood Discards - frames discarded on this port due to Flood limiting. Flooding of received frames with an unknown destination address is 5 frames per second.

Total Discards - total frames discarded on this port.

Transmit Filtered - frames that were not forwarded on this port due to action of one of the 'type' filters.

Blocked or Discarded - frames that were dropped and not delivered on this port. The purpose of this counter is to attempt to count frames which are dropped by the high level WAN driver inside of the unit. This counter will tick when a frame is delivered toward a WAN port, but that port cannot deliver the frame because the port is down or congested.

Forwarded - frames forwarded to a destination on this port.

Flooded - frames transmitted on this port that were broadcast (flooded) to a destination with an unknown location.

Total Forwarded - frames forwarded on this port.

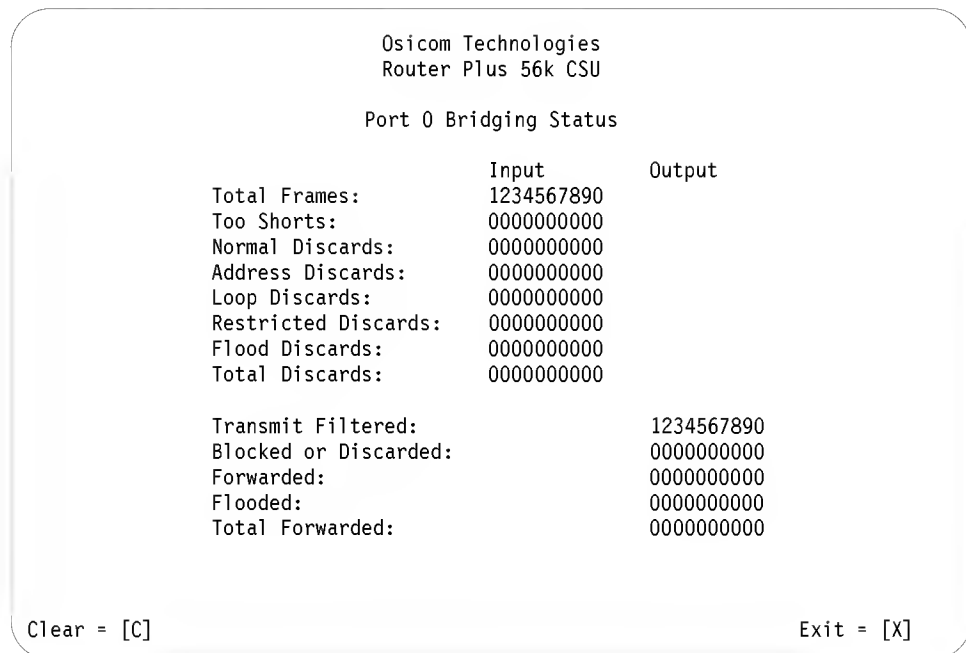
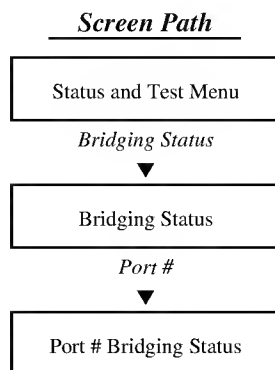


Figure 4-37. Port Bridging Status

4.10 IP Routing Table

Access the IP Routing Table (Figure 4-38) to view all of the known destination networks. All fields are read only. Static routes are configured from the IP Global Configuration screen (see Chapter 5).

The IP routing table contains the information used to decide where to forward IP packets. If RIP (Routing Information Protocol) is enabled, this data is exchanged with adjacent routers.

For both RIP v1 and RIP v2, subnet routes are only advertised on ports that are on the same subnetted network. Subnet routes are hidden or summarized when advertised on a port that is on a different network. Host routes are not supported; any host routes received are discarded.

This screen is updated every 30 seconds. Press **[CR]** to update the screen manually. The routes are listed in numerical order.

Page Down/Page Up prompts appear when there is more than one page of entries.

Type **[F]** to delete all learned entries.

Destination - when an IP packet to be routed is received, its destination address is compared to the destination address in the routing table. The matching entry in the table is used to determine which port the packet will be forwarded on.

If no matching destination address is found in the IP routing table, the packet is sent to the default route address. The default route address is configured at the IP Global Configuration screen. If no default route address is configured, the packet is discarded.

Configure the destination address for a static entry at the Global IP Static Route screen. Configure the destination address for a direct entry at the Port IP Routing Options screen. The destination address for a RIP entry is learned from the value contained in the RIP update message.

Subnet Mask - this is used in conjunction with the destination address to indicate if the route is a network, subnetwork, or host route. Configure the subnet mask for a direct entry at the Port IP Routing Options screen. Configure the subnet mask for a static entry at the Global IP Static Route screen.

The subnet mask for a RIP v1 entry is the default address class mask unless the entry is for the subnet that the router is directly connected to.

The subnet mask for a RIP v2 entry is the mask specified in the routing message.

Screen Path

Status and Test Menu

IP Routing Table

▼

IP Routing Table

Osicnet Technologies
Router Plus 56k CSU

IP Routing Table - Page 1

Destination	Subnet Mask	Next Hop	Hops	Port	Type	Age
118.0.0.0	255.0.0.0		1	2	Dir	
117.0.0.0	255.0.0.0		1	3	Dir	
128.0.0.0	255.255.0.0	118.0.0.12	2	2	RIPv1	10
129.102.0.0	255.255.0.0	118.0.0.12	4	2	RIPv1	20
139.102.0.0	255.255.0.0	118.0.0.12	5	2	RIPv1	12
149.102.0.0	255.255.0.0	118.0.0.12	14	2	RIPv1	26
159.102.0.0	255.255.0.0	118.0.0.12	4	2	RIPv1	5
169.102.0.0	255.255.0.0	118.0.0.12	9	2	RIPv1	1
105.0.0.0	255.0.0.0	117.0.0.101	2	3	Stat	
108.0.0.0	255.0.0.0	117.0.0.101	2	3	Stat	

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Flush = [F]

Update = [CR]
Exit = [X]

Figure 4-38. IP Routing Table

Next Hop - the address of another router that leads to the destination network. The Next Hop address for a Direct route is blank since packets destined for a directly-connected network do not need to be sent to another router, they are delivered to the ultimate destination by the router.

The Next Hop address for a Static route that points out the LAN is configured in the IP Static Route Table screen. The Next Hop address is set to 0.0.0.0 for static routes that point towards the WAN for Unnumbered Mode and Numbered Mode.

The Next Hop address for a RIPv1 route learned from the LAN or a WAN in numbered mode is the source address of the packet the routing message was received from.

The Next Hop address for a RIPv2 route learned from the LAN or a WAN in numbered mode is the address specified in the routing message. If this address is not valid or 0.0.0.0, then the Next Hop address is the source address of the packet the routing message was received from.

The Next Hop address is set to 0.0.0.0 for a RIPv1 route learned on a WAN in Unnumbered Mode.

The Next Hop address for a RIPv2 route learned from a WAN in unnumbered mode is the address specified in the routing message.

Hops - this field indicates how many hops (intervening routers) it takes to reach the destination network. If multiple routes to a network are received, the Routermate Plus will select (learn) the one with the lowest number of hops. The Hops value for a Direct entry is configured on the Port IP Routing Options screen. The Hops value for a Static entry is configured on the IP Static Route Table screen. The Hops value for a RIP entry is the sum of the metric value configured for the port that the routing update message was received on and the metric value reported in the routing update message. The Hops value advertised is equal to the value shown. (Range is 1 - 16)

Port - the port used to reach the destination network.

The port for a direct entry is determined by which port the destination address is associated with. The port for a static entry is determined by which port is entered on the Static Route configuration screen. The port for a RIP entry is the port that received the RIP update message.

Type - specifies the location of the destination network, whether it was configured or learned, and the route's status.

Dir (Direct) - the local router is directly connected to the destination network. Direct routes are configured at the Port IP Routing Options screen.

Stat (Static) - a route to a remote destination network; this route is configured in the local router and overrides RIP routes. Configure static routes on the Global IP Static Route screen.

RIPv1 or RIPv2 (Routing Information Protocol) - a route to a remote destination network; the route was learned from a RIP update message. The RIP version number (v1 or v2) indicates the version of routing update message the route was learned from.

INV (Invalid) - the garbage collection timer is running and the route is in the process of being deleted. The metric is always 16 for an invalid route.

Age - (range 1-999 seconds) the Age field counts the number of seconds since the last update for each RIP entry in the routing table. When an update is received, the Age field is reset to zero. When the Age reaches a value equal to the RIP Route Aging Timer the metric changes to a value of 16. When the Age reaches a value equal to the RIP Route Delete Delay Timer the entry is deleted from the routing table.

When the aging timer reaches 180 seconds, the metric for the route is set to 16, which results in the destination being advertised as un-reachable. If the aging timer reaches a value equal to an internal delete-delay timer (120-second 'Garbage Collection Timeout' the entry is deleted from the routing table.

4.11 IPX Routing Table

Access the IPX Routing Table (Figure 4-39) to view all of the known destination networks. All fields are read only.

The IPX routing table contains information used to decide where to forward IPX packets. This information is also exchanged with adjacent routers using the IPX Routing Information Protocol (RIP).

The routes are listed in numerical order. This screen is updated every 30 seconds. Press **[CR]** to update the screen manually.

Page Down/Page Up prompts appear when there is more than one page of entries.

Type **[F]** to delete all learned entries.

Destination - the 32-bit hex IPX network number for the network that can be accessed. When an IPX packet to be routed is received, its destination address is compared to the destination address in the routing table. The matching entry in the table is used to determine which port the packet will be forwarded on.

If no matching destination address is found in the IPX routing table, the packet is discarded.

Configure the destination address for a direct entry at the Port IPX Routing Options screen. The destination network for a RIP entry is learned from the value contained in the RIP update packet.

Screen Path

Status and Test Menu

IPX Routing Table

▼

IPX Routing Table

Osicom Technologies
Router Plus 56k CSU

IPX Routing Table - Page 1

Destination	Next Hop	Hops	Delay	Port	Type	Age
ABC00001		0	11	0	Dir	
ABC00002		0	11	1	Dir	
ABC00003	ABC00001.08000E000123	10	11	0	RIP	30
ABC00004	ABC00001.08000E000123	10	11	0	RIP	1115
ABC00005	AC000002.000000012e21	10	11	1	RIP	30
ABC00006	AC000002.000000012e21	10	65535	1	RIP	1115

Page Down = **[+]**

Page Up = **[-]**

Flush = **[F]**

Update = **[CR]**

Exit = **[X]**

Figure 4-39. IPX Routing Table

Next Hop - hex address of the next router in the path to the destination network in the form of 32-bit network number plus 48-bit node number. The Next Hop address for a Direct entry is blank since packets destined for a directly-connected network do not need to be sent to another router, they are delivered to the ultimate destination by the router. The Next Hop address for a RIP entry learned from the LAN or a WAN in numbered mode or unnumbered mode is the source address of the packet the routing message was received from.

Hops - this field indicates how many hops (intervening routers) it takes to reach the destination network. The range is 1 - 16. The hops value for a direct entry is 0. The hops value for a RIP entry is the value reported in the routing update message. The hops value advertised is equal to the value displayed, plus 1.

Delay - indicates an estimate of how much time, in ticks, that a 576-byte packet takes to reach the destination network. If multiple routes to a network are received, the Routermate Plus will select (learn) the one with the lowest number of ticks. If two routes exist with equal ticks, the route with the lowest number of hops will be selected. A time tick is approximately 1/18 second or 55ms. The range is 1 - 65535.

The Delay value for a LAN directly-connected route is configured by the Transport Time parameter on the Port IPX Routing Options screen (see page 29).

The Delay value for a WAN directly-connected route depends on the setting of the IPXWAN option parameter on the Port IPX Routing Options screen. If IPXWAN is disabled (default), then the value configured by the Transport Time parameter on the Port IPX Routing Options screen is displayed. If IPXWAN is enabled, then the value calculated by IPXWAN is displayed.

The delay value for a RIP entry is equal to the value reported in the routing update message. The delay value advertised is equal to the value displayed plus the delay for the port it is advertised out.

Port - the port used to reach the destination network. The port for a direct entry is determined by which port the destination address is associated with. The port for a RIP entry is the port on which the RIP update packet was received.

Type - the type specifies the location of the destination network. Valid options:

Dir (Direct) - the local router is directly connected to the destination network. Direct routes are configured at the Port IPX Routing Options screen.

RIP (Routing Information Protocol) - a route to a remote destination network; the route was learned from a RIP update packet.

Age - the number of seconds since the last RIP update packet was received for each RIP entry in the routing table. When a RIP update packet is received, the timer for the age field is reset to zero. When the aging timer reaches the time configured for the **RIP Age Timer** at the Port IPX Routing Options screen, the entry is deleted from the routing table. The default is 180 seconds.

4.12 IPX Services Table

Access the IPX Services Table (Figure 4-40) to view all of the known servers. SAP (Service Advertising Protocol) is an IPX protocol that is used to advertise various Novell application services offered by such devices as file servers and printer servers. Routers exchange service information, which is added to each router's service table. The service table is used to inform the clients about the available servers.

This screen is updated every 30 seconds. Press **[CR]** to update the screen manually.

Page Down/Page Up prompts appear when there is more than one page of entries.

Type **[F]** to delete all learned entries.

Type - a 16-bit (4-character) hexadecimal value representing the type of service. Each server type is identified by a value assigned by Novell. There are values for standard types such as *file server* and *print server*, and for proprietary vendor's equipment such as *HP Laserjet*.

Server Name - a unique 48-character name assigned to the server type (e.g., *file server*, *print server*, *print queue server*).

The router retrieves this name from the incoming SAP update packet and displays the first 24 characters.

Server Address - the full IPX address of the destination server, in the form (hex):

32-bit network : 48-bit Node address : 16-bit Socket

This information is obtained from the incoming SAP update message.

Hops - the number of intervening routers to the destination service. The value displayed is equal to the value reported in the SAP update message. The hops value advertised is equal to the value displayed, plus 1.

Port - number for the port on which the SAP update message was received.

Age - the number of seconds since the last SAP update packet was received for each entry in the table. When a SAP update packet is received, the timer for the age field is reset to zero. When the aging timer reaches the time configured for the **SAP Age Timer** at the Port IPX Routing Options screen (default is 180 seconds), the entry is deleted from the IPX Services Table.

Screen Path

Status and Test Menu

IPX Services Table

▼

IPX Services Table

Osicom Technologies
Router Plus 56k CSU

IPX Services Table - Page 1

Type	Server Name	Server Address	Hops	Port	Age
1234	12345678901234567890	ABCD0003:08000E000123:00E1	1	0	22
104C	12345678901234567890	ABCD0003:08000E000123:00E1	10	1	10
104D	1234567890123456789012345	ABCD0003:08000E000123:00E1	10	1	999

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Flush = [F]

Update = [CR]
Exit = [X]

Figure 4-40. IPX Services Table

4.13 Bridging Table

Access the Bridging Table (Figure 4-41) to display all learned and static MAC addresses for all ports for which bridging is enabled.

This screen is updated every 30 seconds. Press **[CR]** to update the screen manually.

Page Down/Page Up prompts appear when there are more than 12 entries in the table.

Press **[F]** to delete all learned entries.

Press **[C]** to reset **Maximum Entries** to the current value.

Type - how the address was entered, as follows:

Static - the address has been manually entered in the bridging Static Address Table.

Learned - the address is automatically learned.

MAC Address - the 48-bit hexadecimal Ethernet address that is permanently assigned to each device communicating on an Ethernet LAN.

Action - how the bridge handles frames that are either destined to, or sourced from, the specified MAC address, as follows:

Filter - all frames to or from the specified MAC address are filtered (not forwarded).

Forward - frames that contain the specified MAC address in the frame's destination field are forwarded to this port; frames that contain the specified MAC address in the source field should be received on this port.

Filtering is configured as a global bridging option in the bridging Static Address Table.

Port - location where frames are forwarded based on their destination address. Frames containing the specified MAC address in the source field will be received on this port. Frames received by the bridge containing the specified MAC address in the destination field will be forwarded to this port. The Port value is ignored and dashes (--) are displayed when the 'Action' is set to *Filter*.

Port numbers either are configured in the Static Address Table or are learned automatically.

Screen Path

Status and Test Menu

Bridging Table

▼

Bridging Table

Osicom Technologies
Router Plus 56k CSU

Bridging Table - Page 1

Type	MAC Address	Action	Port
Static	00:00:6d:00:30:00	Filter	--
Static	00:00:6d:00:30:01	Filter	--
Static	00:00:6d:00:30:02	Forward	2
Static	00:00:6d:00:30:03	Forward	1
Learned	00:00:6d:00:30:04	Forward	1
Learned	00:00:6d:00:30:05	Forward	1
Learned	00:00:6d:00:30:06	Forward	1
Learned	00:00:6d:00:30:07	Forward	1
Learned	00:00:6d:00:30:08	Forward	1
Learned	00:00:6d:00:30:09	Forward	1
Learned	00:00:6d:00:30:10	Forward	1
Learned	00:00:6d:00:30:11	Forward	1

Current Entries: 0020
Maximum Entries: 0035

Page Up = [-]
Page Down = [+]

Clear = [C]
Flush = [F]

Update = [CR]
Exit = [X]

Figure 4-41. Bridging Table

4.14 Event Log

The Event Log screen (Figure 4-42) records all statistical and error messages that occur during startup and operation. The maximum number of events is 45. The most recent event is shown first.

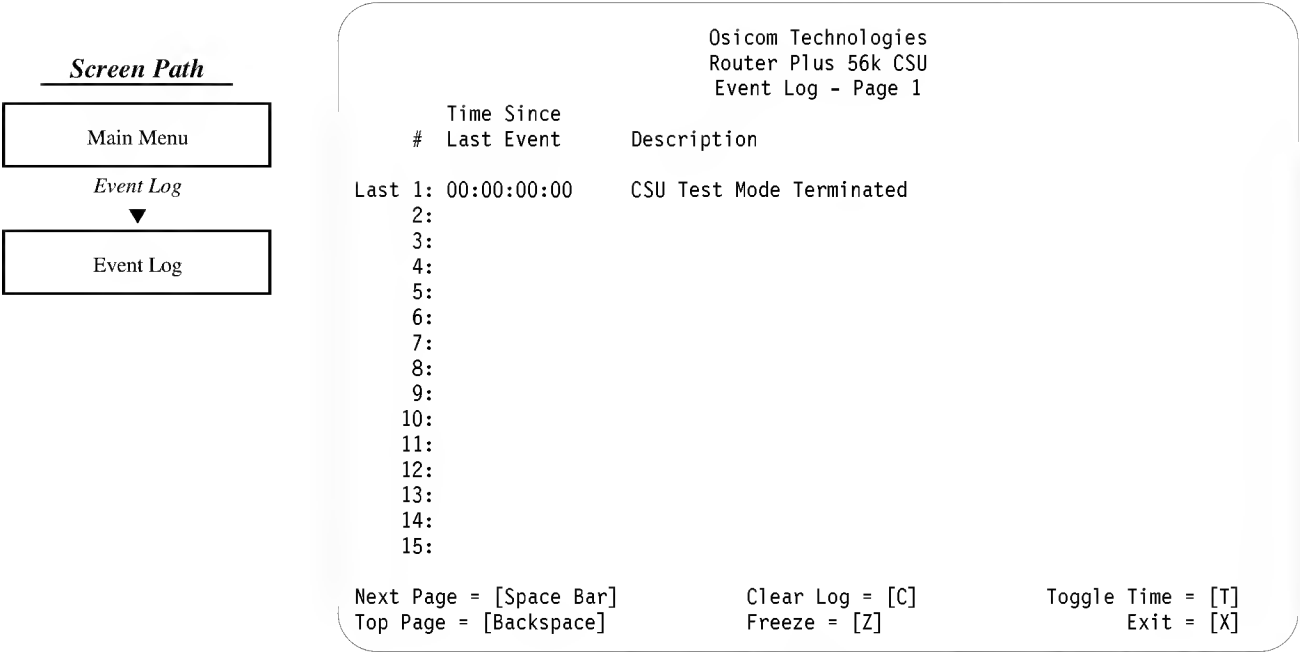


Figure 4-42. Event Log

This chapter illustrates and describes the router's configuration screens. Access these screens to configure the router's operational parameters to suit your application. This text also serves as a reference tool for defining the parameters and options displayed on the screens.

After reading this chapter, the user will be able to locate specific configuration screens and understand the contents and purpose of each.

5.1	Screen Structure	5-2
5.2	Configuration Menu	5-5
5.3	CSU Configuration	5-6
5.4	Interface Configuration Summary ..	5-7
5.4.1	LAN Configuration	5-8
5.4.2	WAN Configuration	5-9
5.4.2.1	WAN Protocol Options (Frame Relay)	5-10
5.5	Port Configuration Summary	5-12
5.5.1	Port Configuration	5-13
5.5.1.1	IP Routing Options (LAN)	5-16
5.5.1.2	IP Routing Options (WAN)	5-19
5.5.1.3	IP Filters	5-21
5.5.1.3.1	IP RIP Input/Output Filters	5-23
5.5.1.4	IPX Routing Options	5-24
5.5.1.5	IPX Filters	5-27
5.5.1.5.1	IPX SAP Input/Output Filters	5-29
5.5.1.5.2	IPX RIP Input/Output Filters	5-32
5.5.1.6	Bridging Options	5-34
5.5.1.6.1	Transmit Filters	5-35
5.5.1.7	Encryption Options (Frame Relay and PPP)	5-37
5.6	Global Configuration	5-39
5.6.1	IP Global Configuration	5-40
5.6.1.1	IP Static Routes	5-42
5.6.1.2	IP RIP Neighbor List Table	5-44
5.6.2	IPX Global Configuration	5-45
5.6.3	Bridging Global Configuration	5-46
5.6.3.1	Bridging Static Addresses	5-48
5.6.4	PPP Global Configuration	5-50
5.6.5	Encryption Global Configuration ..	5-51

5.1 Screen Structure

The organization of the **Configuration** screens is shown below.

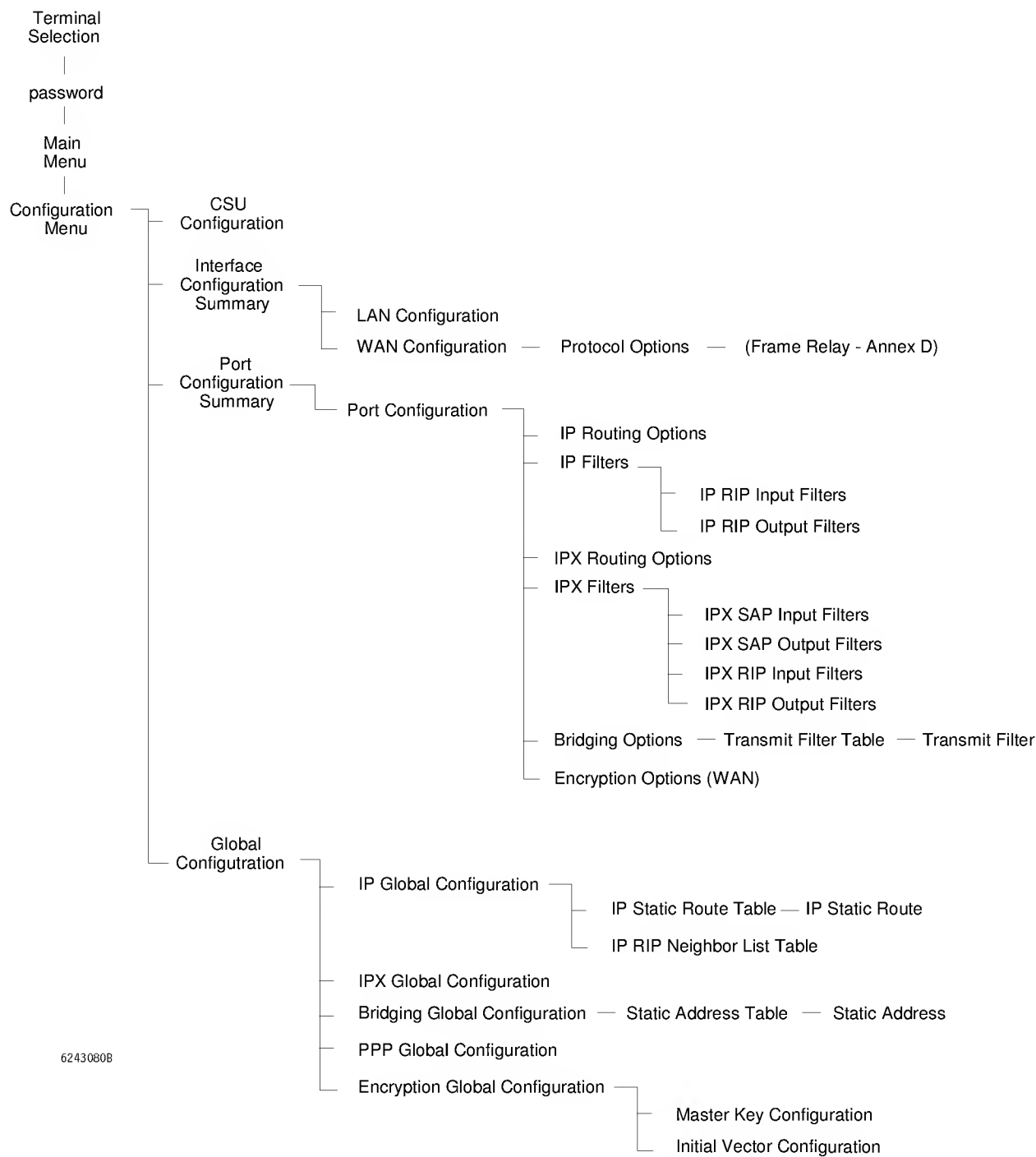


Figure 5-1. Screen Structure (Configuration)

For convenience, the Routermate Router Plus 56K CSU separates configuration parameters into four areas:

- *CSU Configuration* (Section 5.3, and following)
- *Interface Configuration* (Section 5.4, and following)
- *Port Configuration* (Section 5.5, and following)
- *Global Configuration* (Section 5.6, and following)

This separation reflects the difference between hardware and software considerations, as follows:

CSU Configuration - applies to parameters for the integral 56 kbps channel service unit.

Interface Configuration - applies to the protocol to be used on the physical interface:

- The LAN interface is permanently configured for Ethernet protocol.
- The WAN interface can be configured for either PPP (Point-to-Point) or Frame Relay. Specific connect service protocol options are configured depending on whether PPP or Frame Relay is selected.

Port Configuration - pertains to the router software, and the configuration of routing, bridging, and filtering options. The router can have up to 15 ports (numbered 0 through 14) as follows:

- Port 0 is permanently mapped to the LAN interface.
- If the WAN interface is configured for PPP, Port 1 is mapped to the WAN interface, and the maximum number of ports is 2 (port 0 and port 1).
- If the WAN interface is configured for Frame Relay service, from one to fourteen Permanent Virtual Circuits (PVCs) are mapped to the WAN interface, and the number of ports equals the number of PVCs plus one additional port (Port 0), which is mapped to the LAN interface.

Global Configuration - involves the configuration of parameters that apply to all configured ports; it is not port-specific.

A brief description of each screen follows.

CSU Configuration - configure parameters for the integral 56K CSU (Channel Service Unit).

Bandwidth Allocation - assign DS0s to the network interface (WAN 1).

Interface Configuration - set parameters for the network interface (WAN 1).

Interface Configuration Summary - view the protocol and condition of the LAN and WAN interfaces. Access the interface-specific screens below.

LAN Configuration - enable/disable the LAN interface; view the local MAC address.

WAN Configuration - enable/disable the WAN interface; access the screens below.

WAN Protocol Options - configure protocol options for the WAN interface (Frame Relay - Annex D only).

Port Configuration Summary - view configuration parameters for all the virtual ports defined on the router; includes port number, name, corresponding interface, protocol, and the type of routing or bridging configured; access the port-specific configuration screens below.

Port Configuration - assign port numbers and corresponding interfaces (WAN only); configure IP, IPX, and bridging options; access IP and IPX Filters screens.

IP Routing Options - configure Internet Protocol options on this port.

IP Filters - configure IP filtering options on this port; access the screens below.

IP RIP Input Filter Table - configure networks that are not allowed to be learned on this port from the routing update packet.

IP RIP Output Filter Table - configure networks that are allowed to be advertised on this port in the routing update packet.

IPX Routing Options - configure IPX options on this port.

IPX Filters - configure IPX filtering options on this port; access the screens below.

IPX SAP Input Filter Table - display services that are not allowed to be learned on this port from Service Advertising Protocol (SAP) routing update packets.

IPX SAP Output Filter Table - display services that are allowed to be advertised on this port in SAP routing update packets.

IPX RIP Input Filter Table - display networks that are not allowed to be learned on this port from IPX Routing Information Protocol (RIP) routing update packets.

IPX RIP Output Filter Table - display networks that are allowed to be advertised on this port in IPX RIP routing update packets.

Bridging Options - enable/disable broadcast, multicast, and filtering options for this port. Access the screen below.

Transmit Filters - configure filtering of specific types of Ethernet frames.

Encryption Options - configure encryption options for the WAN interface.

Global Configuration - access the global configuration screens below.

IP Global Configuration - configure global IP parameters.

IP Static Route Table - view static routes configured on the IP Static Route screen.

IP Static Route - configure a user-defined route to a router or network in the IP Routing Table.

IP RIP Neighbor List Table - view and configure addresses of directly-connected routers (any adjacent router) from which IP RIP update packets will be accepted.

IPX Global Configuration - configure global IPX parameters.

Bridging Global Configuration - configure global bridging parameters. Access the screen below.

Static Address Table - view and delete specific addresses for forwarding or filtering.

Static Address - add or edit an entry in the Static Address Table.

PPP Global Configuration - configure global PPP (Point-to-Point Protocol) parameters.

Encryption Global Configuration - configure the Key Update Time for the Pending Key configured on the port-specific Encryption Configuration screen.

5.2 Configuration Menu

Access the Configuration Menu (Figure 5-2) from the Main Menu. This is the top-level menu from which you select other screens to configure parameters for the integral CSU and the LAN and WAN interfaces.

To make a selection:

1. Press the **[Space Bar]** or **[Backspace]** to move the cursor to the desired selection.
2. Press **[CR]**; the selected menu appears.

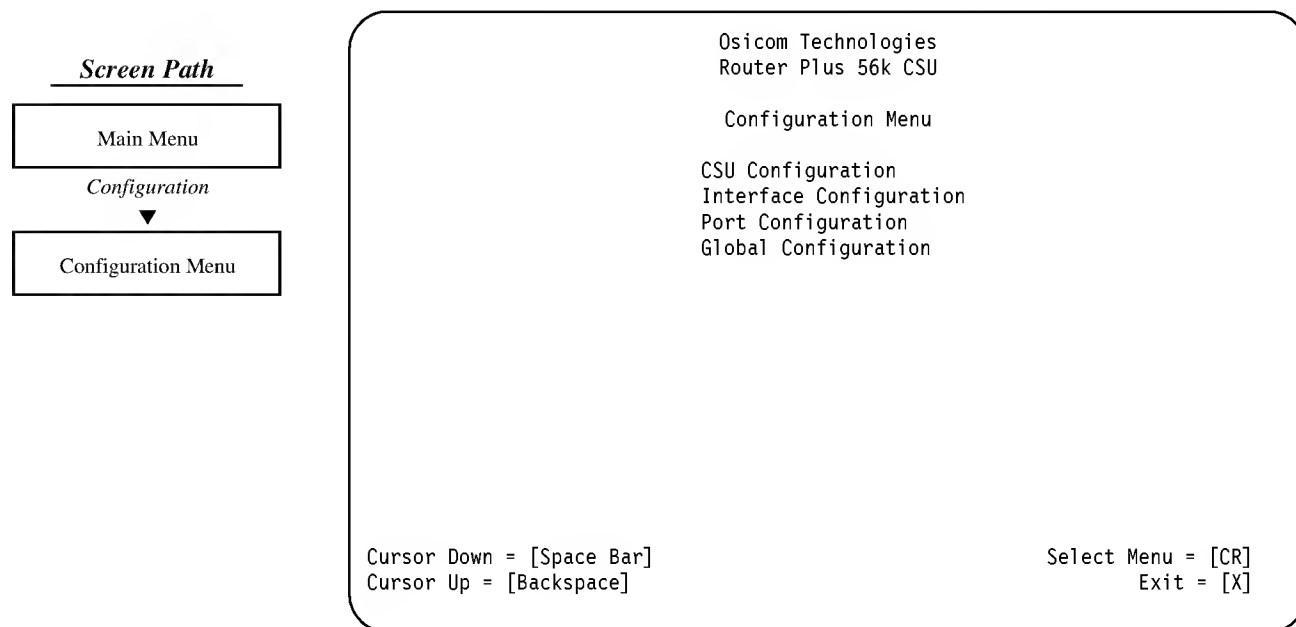


Figure 5-2. Configuration Menu

5.3 CSU Configuration

Access the CSU Configuration screen (Figure 5-3) to configure parameters for the integral 56K CSU. Position the cursor at the parameter you want to change, then press **[CR]** to scroll through the options.

Timing - the network transmit and receive clock.

Internal - the CSU provides both transmit and receive clocks; choose Internal if you are using the Routermate Plus as a Limited Distance Modem (LDM). In LDM mode, always set one end to *Internal* and the other end to *Repeater* timing.

NOTE

In this mode, only the end set to *Internal* timing can initiate an RDL test.

Repeater - the Routermate Plus frequency-locks its transmit clock to its receive clock. When the CSU is attached to a DDS network, set each end to *Repeater* Timing.

Default: *Repeater*

Respond to RDL - enable/disable the CSU's ability to *respond* to a remote digital loopback request from the remote end (not the ability to generate the loopback request).

Default: *Enabled*

Screen Path

Configuration Menu

CSU Configuration



CSU Configuration

Osicom Technologies
Router Plus 56K CSU

CSU Configuration

Timing:

Respond To RDL:

Repeater

Enabled

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Select = [CR]
Exit = [X]

Figure 5-3. CSU Configuration

5.4 Interface Configuration Summary

Access the Interface Configuration Summary screen (Figure 5-4) to view the protocol configuration on the router's LAN and WAN interfaces.

To reconfigure an interface, position the cursor on the desired interface and press **[CR]**; that interface's configuration screen is displayed.

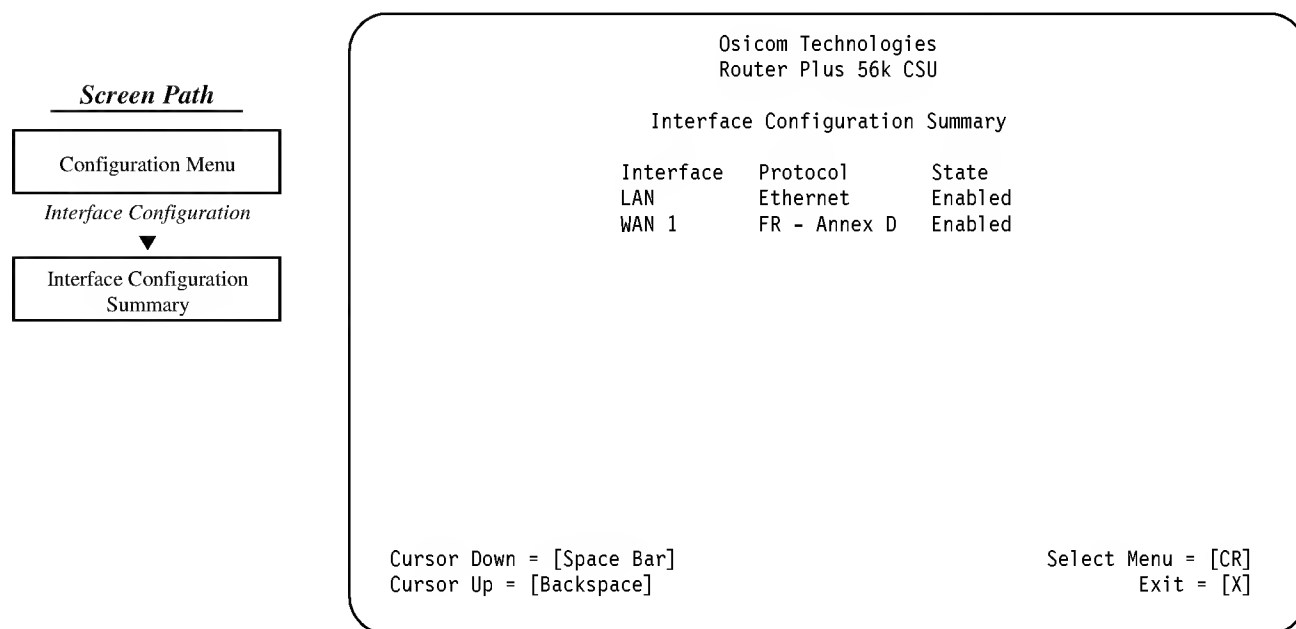


Figure 5-4. Interface Configuration Summary

5.4.1 LAN Configuration

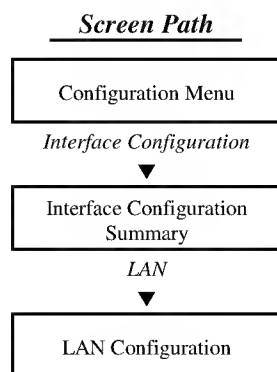
Access the LAN Configuration screen (Figure 5-5) to enable or disable the Local Area Network (LAN) interface and display the interface protocol and MAC Address. The LAN interface is the rear-panel interface labeled 10BaseT.

State - enable/disable the LAN interface.

Default: *Enabled*

Protocol - the LAN interface protocol is permanently configured for *Ethernet*.

MAC Address - this read-only field displays the 48-bit hexadecimal Media Access Control (MAC) address. The MAC address is permanently assigned to the LAN interface.



Osicom Technologies
Router Plus 56k CSU

LAN Configuration

State: Enabled

Protocol: Ethernet

MAC Address: FF:FF:FF:FF:FF:FF

Select = [CR]
Exit = [X]

Figure 5-5. LAN Configuration

5.4.2 WAN Configuration

Access the WAN 1 Configuration screen (Figure 5-6) to configure the state and protocol of the Wide-Area Network (WAN) interface. The WAN interface is the rear-panel interface labeled WAN 1.

To configure protocol options, position the cursor on **Protocol Options** and press **[CR]**; the protocol options screen for the selected protocol is displayed.

NOTE

Protocol Options is only displayed when WAN 1 is configured for Frame Relay - Annex D.

State - enable/disable the WAN 1 interface.

Default: *Enabled*

Protocol - configure the protocol on the WAN 1 interface. Select:

PPP (sync)

Frame Relay - Annex D

Frame Relay - No LMI

The router supports IP Routing, IPX Routing and Transparent Bridging over PPP or Frame Relay.

The PPP LCP RFC1661, IPCP RFC1332, IPXCP RFC1552, and BCP RFC1638 are supported.

The router treats Frame Relay as a series of point-to-point connections. In **Numbered** mode, each port must be assigned a unique network or sub network number. RFC1490 and Cisco frame relay encapsulations are supported for IP Routing, IPX Routing, and Transparent Bridging. Osicom's 4802 Bridging Frame Relay encapsulation is also supported.

Inverse ARP is supported to provide compatibility with other vendor's routers that require Inverse ARP.

CRC recalculated mode is used for bridging over PPP and Frame Relay (RFC1490 and Cisco Encapsulation). CRC pass-through is not supported.

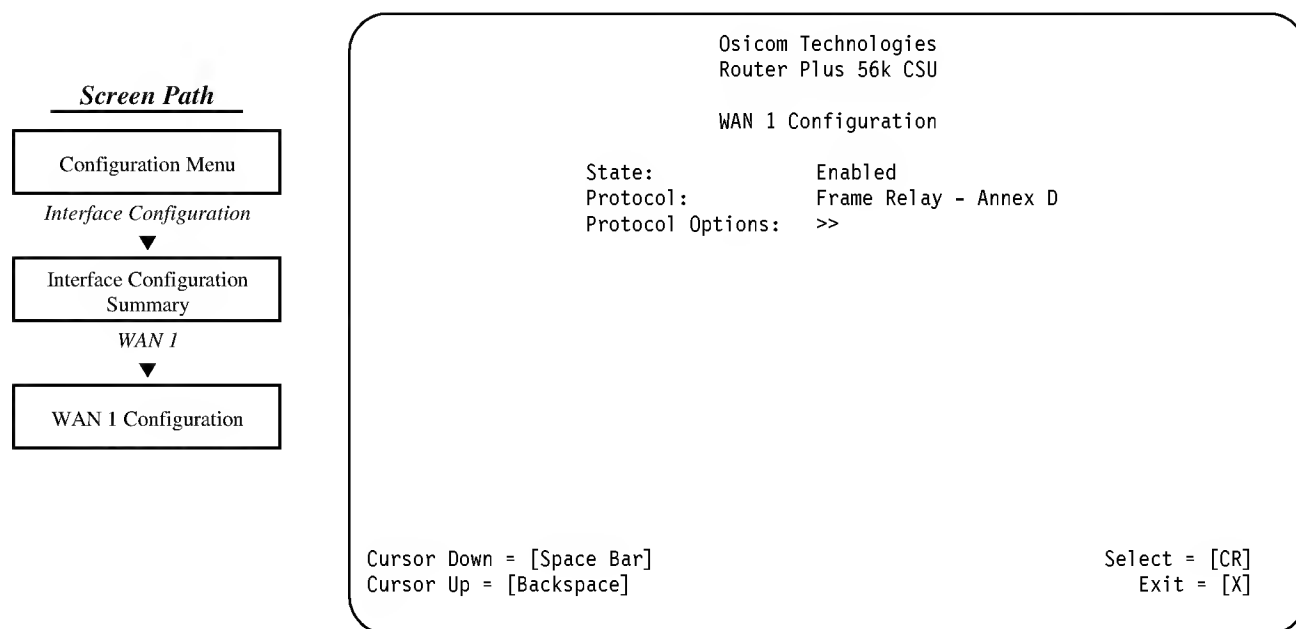


Figure 5-6. WAN Configuration (Frame Relay)

Protocol (cont)

PPP (sync) - Point-to-Point Protocol, in accordance with RFC 1548, provides a standard method for transporting multi-protocol datagrams over point-to-point links.

Frame Relay - Annex D - uses the protocol defined by the American National Standards Institute (ANSI) publication *T1.617, Annex D*. Select this option when the WAN interface is connected to a frame relay service.

Frame Relay - No LMI - a Frame Relay protocol without Local Management Interface (LMI). Select this option for back-to-back testing.

NOTE

Frame Relay - No LMI is used primarily for test purposes.

Default: *PPP (sync)*

5.4.2.1 WAN Protocol Options (Frame Relay)

Access the WAN 1 Protocol Options screen to configure protocol options for the WAN interface. WAN protocol options only apply if the protocol is set for Frame Relay - Annex D.

The counters configured at this screen relate to frame relay polling and polling responses over the WAN link. Normally, these parameters can be left at their recommended default settings. The settings can be increased by a knowledgeable user who wishes to decrease WAN link overhead.

Full Enquiry Interval - the frequency at which the unit requests full status information relative to the number of regular status requests. With the default setting of 6, for example, 1 of every 6 status requests is a request for full status.

Valid range: 1 - 255

Default: 6

Error Threshold - number of either Local In-channel Signalling Link Reliability Errors or Local In-channel Signalling Protocol Errors that can occur during a sliding monitored events count defined by **Monitor Events** (see following parameter) before a channel or frame relay user device is declared inactive.

The value of this parameter must be less than the value for **Monitored Events**; entering a higher value is not permitted.

Valid range: 1 - 10

Default: 3

Monitor Events - count of monitored events (in number of messages). From the router's perspective, a monitored event is the transmission of a poll for status (see **Polling Interval**, following).

Monitor Events specifies the size of the sliding window used by the router to determine whether a channel or user device is active. After a channel or user device is declared inactive, the router waits the specified number of successful poll cycles before declaring the channel/user device active again. The user device can also wait the specified number of successful poll cycles to detect service restoration.

The value of this parameter must be greater than the value of the **Error Threshold** parameter; entering a lower value is not permitted.

Valid range: 2 - 11

Default: 4

Polling Interval - the frequency at which the network is polled for status. This setting must be smaller than the setting for **Polling Verification Timer Interval**; entering a higher value is not permitted.

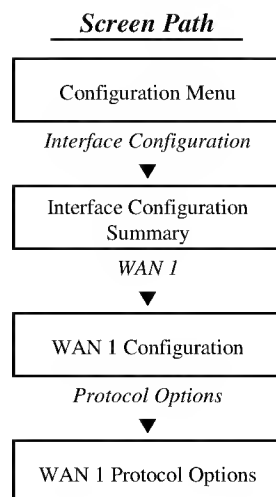
Valid range: 5 - 30 seconds

Default: 10 s

Polling Verification Timer Interval - the timer for verifying the polling cycle. This setting must be greater than the setting for **Polling Interval**; entering a lower value is not permitted.

Valid range: 6 - 31 seconds

Default: 15 s



```

Osicom Technologies
Router Plus 56k CSU

WAN 1 Protocol Options

Full Enquiry Interval:      6
Error Threshold:           3
Monitor Events:            4
Polling Interval:          10 s
Polling Verification Timer Interval: 15 s

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Edit Field = [CR]
Exit = [X]
  
```

Figure 5-7. WAN Protocol Options (Frame Relay)

5.5 Port Configuration Summary

Access the Port Configuration Summary screen (Figure 5-8) to view information about all the ports configured on the router. The maximum number of ports is 15, (1 for LAN and 14 for WAN 1).

To configure a specific port:

1. Position the cursor on the desired port number and press **[CR]**.
2. The Port Configuration screen for the selected port is displayed.

The contents of the Port Configuration screen for an individual port depends on the protocol selected.

Port - displays the port number.

- Port 0 is always the LAN interface (the rear-panel interface labeled 10BaseT).
- If the WAN 1 interface is configured for PPP, Port 1 is mapped to the WAN 1 interface.
- If the WAN 1 interface is configured for Frame Relay, from 1 to 14 Permanent Virtual Circuits (PVCs) can be mapped to the WAN 1 interface.

Port Name - free-text port identifier configured at the Port Configuration screen (see following section).

Interface - interface (LAN or WAN) to which each port is mapped at the Port Configuration screen.

Protocol - the protocol used for the port (Ethernet, PPP, or FR). The protocol for the LAN interface (Port 0) is always Ethernet. The protocol for the WAN interface (ports 1 through 14) is configured at the WAN Interface screen.

If the protocol is either *Frame Relay - Annex D* or *Frame Relay - No LMI*, the unit displays **FR** followed by the DLCI (Data Link Connection Identifier) for this port. The DLCI is configured at the Port Configuration screen. The default DLCI is 25.

Route/Bridge - the method of routing or bridging that has been enabled at the Port Configuration screen for this port:

IP - IP routing

IPX - IPX Routing

BR - Bridging

Screen Path

Configuration Menu

Port Configuration

▼

Port Configuration Summary

Osicom Technologies
Router Plus 56k CSU

Port Configuration Summary

Port	Port Name	Interface	Protocol	Route/Bridge
0	Local Site	LAN	Ethernet	IP IPX BR
1	Remote Site 1	WAN 1	FR-1000	BR
2	Remote Site 2	WAN 1	FR-1001	IP IPX
3	Remote Site 3	WAN 1	FR-1002	IP
4	Remote Site 4	WAN 1	FR-1003	IP
5	Remote Site 5	WAN 1	FR-1004	IP
6	Remote Site 6	WAN 1	FR-1005	IP
7	Remote Site 7	WAN 1	FR-1006	IP
8	Remote Site 8	WAN 1	FR-1007	IP
9	Remote Site 9	WAN 1	FR-1008	IP
10	Remote Site 11	WAN 1	FR-1009	IP
11	Remote Site 11	WAN 1	FR-1010	IP
12	Remote Site 12	WAN 1	FR-1011	IP
13	Remote Site 13	WAN 1	FR-1012	IP
14	Remote Site 14	WAN 1	FR-1013	IP

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Select Menu = [CR]
Exit = [X]

Figure 5-8. Port Configuration Summary

5.5.1 Port Configuration

Use the Port Configuration screen to identify the port and to enable or disable the following:

- IP routing
- IPX routing
- Filtering
- Bridging
- Encryption (WAN only)

Configuration options for ports mapped to the LAN and WAN interfaces are identical except for the parameters noted. Figure 5-9 shows the screen for Port 0 (LAN). When Frame Relay is selected for the WAN interface, the additional options noted in Figure 5-10 are displayed.

To access any of the options screens, position the cursor on the desired selection and press **[CR]**.

Port Name - a text name for this port.

Valid input: Maximum 24 alphanumeric characters.

Interface - the interface to which this port is mapped.

Valid input: *LAN*, *WAN 1* or *None*. Selecting *None* blanks out all columns on the Port Configuration Summary screen.

Default: Port 0 = *LAN*
 Port 1 = *WAN 1*
 Ports 2-14 = *None*

IP Routing - enable/disable IP routing on this port.

Default: *Enabled*

IPX Routing - enable/disable IPX routing on this port.

Default: *Disabled*

Bridging - enable/disable bridging on this port.

Enabled - incoming frames that are not routed are bridged.

Disabled - incoming frames that are not routed are discarded.

Default: *Disabled*

Port State (Frame Relay only) - enable/disable this port.

Default: *Enabled*

DLCI (Frame Relay only) - set the Data Link Connection Identifier for this port (provided by carrier).

Valid range: *0 - 1023*

Default: *25*

Encapsulation - This option is only displayed if the WAN protocol is set to Frame Relay (No LMI or Annex D).

RFC1490 - the router will receive IP routed, IPX routed, and bridged frames over frame relay in both RFC1490 and Cisco encapsulation. The router automatically changes the transmit encapsulation depending on the encapsulation received. Upon power up or link up, the router will default to transmitting in RFC1490 encapsulation. Upon receipt of a Cisco encapsulated frame, the router will automatically switch to transmitting in the Cisco encapsulation.

RFC4802 - the bridged traffic will be encapsulated in the 4802 format allowing interoperability with older 4802s that do not support RFC1490 encapsulation.

Default: *RFC1490*

Encryption - enable/disable encryption on this port.

NOTE

Encryption and **Encryption Options** are only displayed when the optional encryption daughter card is installed.

For units that include optional encryption hardware, the Encryption Options screen cannot be accessed and encryption options cannot be configured unless the **Key Password** is entered at the Password screen. This applies to terminal or Telnet access.

Default: *Disabled*

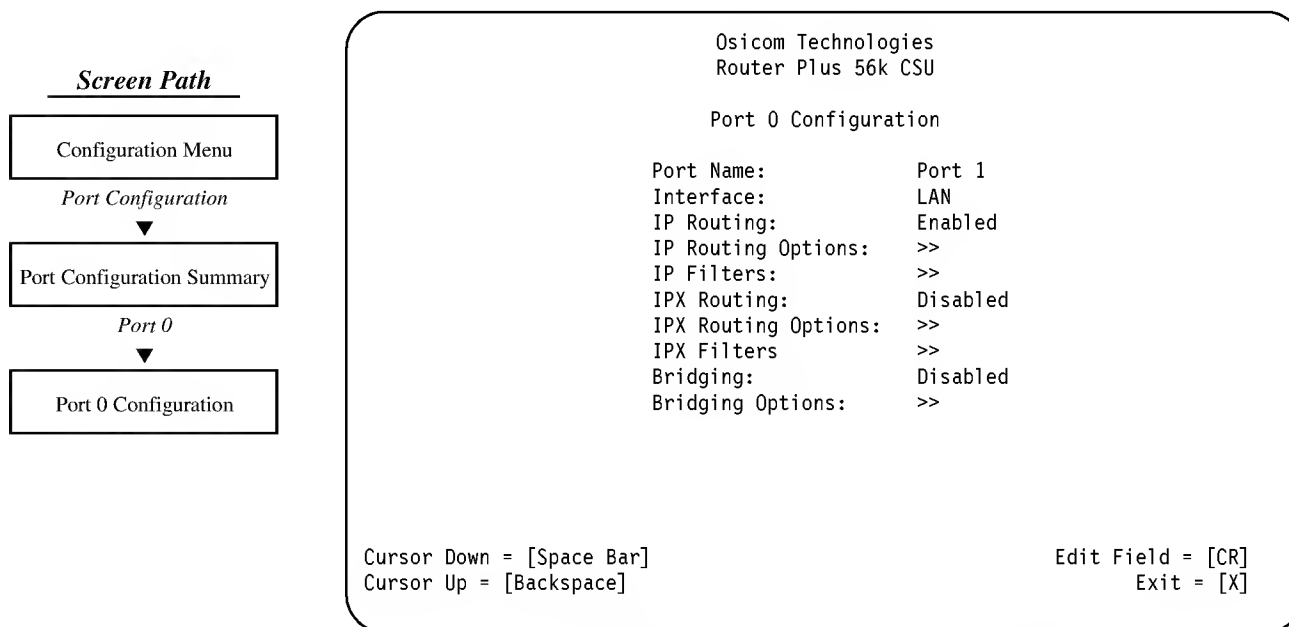


Figure 5-9. Port 0 Configuration (LAN)

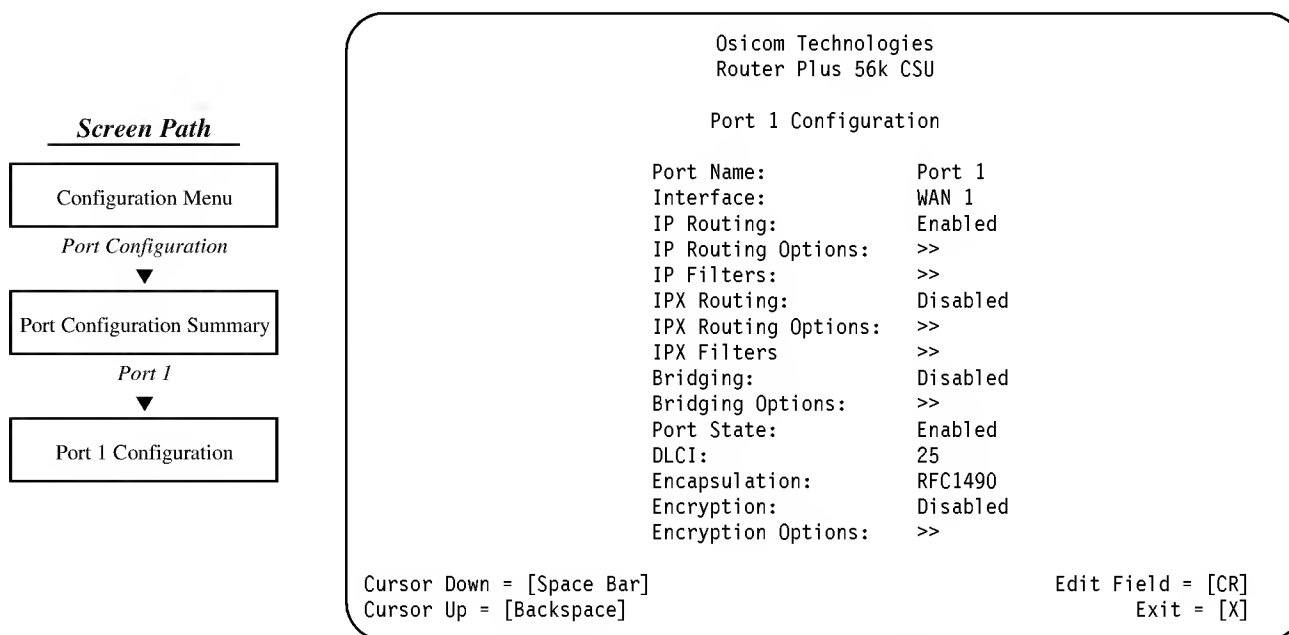


Figure 5-10. Port 1 Configuration (WAN; Frame Relay)

5.5.1.1 IP Routing Options (LAN)

Access the Port IP Routing Options screen (Figure 5-11) to configure IP routing options for port 0 (LAN).

Address - the Internet Protocol (IP) address for this port expressed in dotted decimal notation. All zeros indicate no address defined.

The Address for each port must have a unique network number. The host portion of the Address can not be set to all zeros. The first and the last network address of each address class are reserved. The valid and invalid address are listed below. The user is not allowed to save changes with a duplicate, all zeros, or invalid address. The "Invalid Address" message is displayed if Yes is entered at the save configuration prompt.

NOTES

The default LAN address will allow a defaulted router to be accessed via its LAN or WAN ports. When defaulted, access via the WAN will require the remote router to be configured for **Unnumbered** links.

The default LAN address is only intended to allow initial Telnet access to the router so that it can be configured without attaching a terminal to the console port. The default address is not intended to be used during normal operation

0.0.0.0	reserved
1.0.0.0 - 126.0.0.0	available
127.0.0.0	reserved

128.0.0.0	reserved
128.1.0.0 - 191.254.0.0	available
191.255.0.0	reserved

192.0.0.0	reserved
192.0.1.0 - 223.255.254.0	available
223.255.255.0	reserved

224.0.0.0 - 239.255.255.255	reserved
240.0.0.0 - 255.255.255.254	reserved
255.255.255.255	reserved

Default: LAN = 192.0.2.1
WAN = 192.0.3.1 (Numbered mode)

Subnet Mask - if IP subnetworking is used, identifies the parts of the IP address that are used for the network, subnetwork, and host numbers.

A mask that is smaller than the default mask value is not permitted but a mask that is larger than default is permitted. The default subnet masks are identified below.

Network Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Default: 255.255.255.0

Setting the subnet portion of the address to all ones is always allowed, but setting the subnet portion of the address to all zeros is only allowed if the global Subnet Zero option is Enabled. Setting the subnet portion of the address to all ones or all zeros is discouraged.

A subnet of all ones broadcast address is the same as the network broadcast address. For example, the broadcast address for network 130.110.0.0 is 130.110.255.255, which is the same as the broadcast address for subnet 130.110.255.0.

A route for a subnet of all zeros has the same address as a network route. For example, if network 130.110.0.0 is subnetted as 255.255.255.0, the subnet zero route would be 130.110.0.0, which is the same as the network route.

RIP - set Routing Information Protocol as described below. The key feature of RIP version 2 is inclusion of the subnet mask with the routing updates. This allows use of variable length subnet mask (VLSM).

Different ports on the router can use different RIP versions. In this case, the router will perform a conversion between the RIP versions. RIP version 2 should be used throughout a subnetted network if VLSM is used since RIP version 1 cannot interpret VLSM routes correctly.

Osicom's implementation of RIP version 2 does not support authentication.

For both RIP v1 and RIP v2, subnet routes are only advertised on ports that are on the same subnetted network. Subnet routes are hidden or summarized when advertised on a port that is on a different network. Host routes are not supported; any host routes received are discarded.

RIP v1 Only - RIP messages are advertised in the v1 format; only v1 format messages are learned. Broadcast and multicast v2 format messages are not learned.

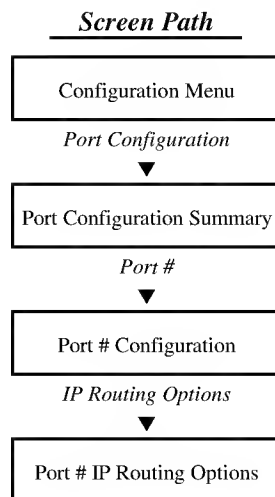
RIP v1 Compatible - the RFC1058 compliant version of RIP. RIP messages are advertised in the v1 format; v1 format messages and v2 format messages that are broadcast are learned. V2 format messages that are multicast are not learned.

RIP v2 Compatible - RIP messages are advertised via broadcast messages in the v2 format. RIP v1 format messages, v2 format messages that are broadcast, and v2 format messages that are multicast are learned.

RIP v2 Only - RIP messages are advertised via multicast messages in the v2 format, and v2 format messages that are multicast are learned. V1 format messages and v2 format messages that are broadcast are not learned.

Disabled - RIP messages are not advertised or learned on this port.

Default: *RIP v1 Compatible*



Osicom Technologies
Router Plus 56k CSU

Port 0 IP Routing Options

Address:	192.0.2.1
Subnet Mask:	255.255.255.0
RIP:	RIP v1 Compatible
Metric:	1
Frame Type:	TYPE II

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Edit Field = [CR]
Exit = [X]

Figure 5-11. Port 0 IP Routing Options (LAN)

Metric - sets the weight (number of hops) associated with this port. This determines the number of hops to enter in the IP Routing Table for the direct entry associated with this port. The metric value is added to the value received in the RIP message and the sum is placed in the IP routing packet for each route learned on this port.

Valid input: *1 to 15*

Default: *1*

Frame Type (LAN only) - the MAC layer frame encapsulation to be used for IP transmissions out the specified port. SNAP is used very seldom since the native frame type for IP is Type II.

Valid input: *Type II or SNAP* (see table below)

Default: *Type II*

Frame Type	MTU
TYPE II	1500
SNAP	1492

5.5.1.2 IP Routing Options (WAN)

Access the Port IP Routing Options screen (Figure 5-12) to configure IP routing options for the WAN interface.

See Port IP Routing Options for the LAN in the previous section for parameters not defined here.

Mode - set the operating mode for this port.

Numbered - an IP address must be assigned to this port.

Unnumbered - no IP network or subnetwork numbers are assigned to the WAN interface. Besides conserving IP address space, Unnumbered mode also decreases the size of the routing table since no direct routes are created for the WAN ports. This reduces the amount of memory required to hold the routing table and also decreases the amount of bandwidth used to send routing updates.

When the mode is changed from Unnumbered to Numbered, the Address and Subnet mask values are displayed. The default value for Port 1 is 192.0.3.1 (255.255.255.0). The default value for Port 2 and greater is 0.0.0.0 255.255.255.0. A direct route for Port 2 and greater is not created until a valid address and subnet mask is entered.

Address and Subnet Mask

- the Address and Subnet Mask values are only displayed if the mode is *Numbered*.

When the mode is *Unnumbered*, the Address and Subnet mask values are blanked out. A direct route for Port 2 and greater is not created until a valid address and subnet mask is entered. The valid values for the address and subnet mask are the same as those defined for port 0.

Defaults:

Port 1: Address - 192.0.3.1
Subnet Mask - 255.255.255.0
Port 2 and greater: Address - 0.0.0.0
Subnet mask - 255.255.255.0

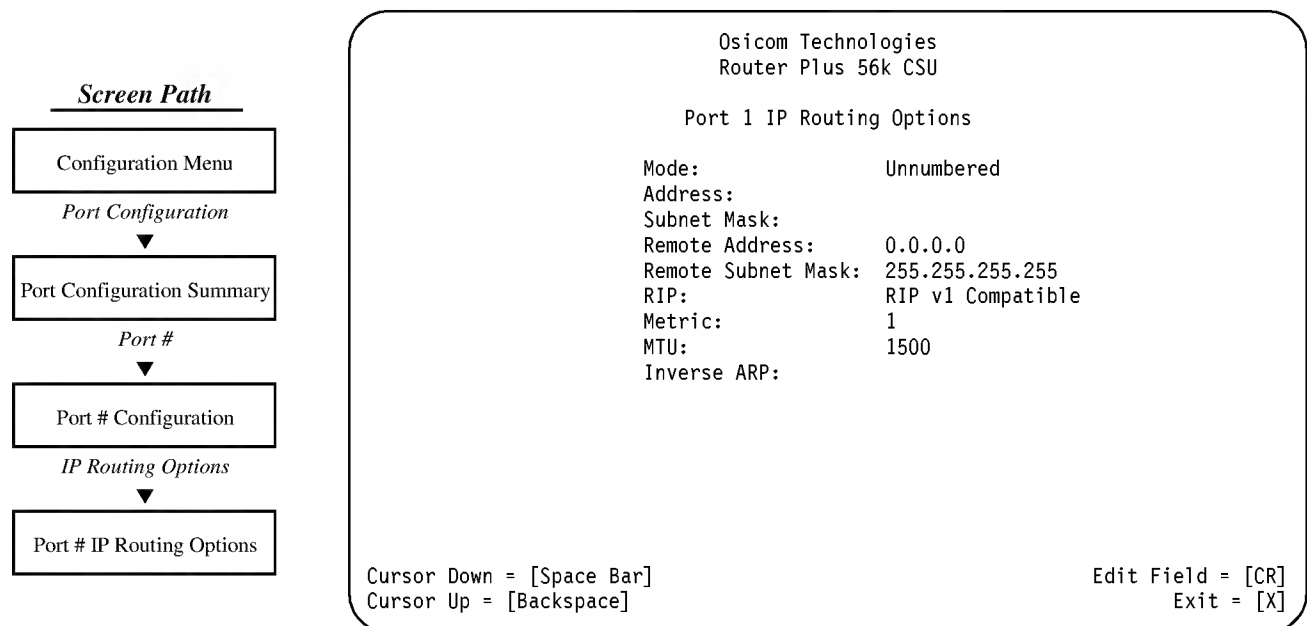


Figure 5-12. Port 1 IP Routing Options (WAN)

Remote Address - determines which subnets should be advertised and learned on this port. Enter the address of the remote router's LAN port (the remote router ID). The Remote Address value is only displayed if the mode is *Unnumbered*. When the mode is *Numbered*, the Address value is blanked out. This option only needs to be configured if subnet routes need to be advertised across an unnumbered link. When left at the default value, all subnet routes will be summarized – only the parent network address of IP subnets are advertised.

Default: 0.0.0.0

Remote Subnet Mask - use this option in conjunction with the Remote Address option to determine which subnets should be advertised and learned on this port. If the routers are on the same network, enter the subnet mask of the remote router's LAN port. If the routers are on different networks, enter the network mask of the remote router's LAN port.

The Remote Subnet Mask value is only displayed if the mode is *Unnumbered* and RIP is set to *RIP v1 Only*, *RIP v1 Compatible*, or *RIPv2 Compatible*. When the mode is *Numbered* or the mode is *Unnumbered* and RIP is *RIP v2 Only*, then the Remote Subnet Mask value is blanked out.

Default: 255.255.255.0

MTU (Maximum Transmission Units) (WAN only) - the maximum permitted size, in bytes, of IP frames to be transmitted out the WAN interface. The MTU includes the size of the IP header and IP data fields.

Valid input: 296, 576, 1492, 1500

Default: 1500

Inverse ARP (WAN only) - applies only if the Protocol is set to Frame Relay (see WAN Configuration screen (Section 5.4.2, page 5-9) and the Mode is *Numbered*. When the Mode is *Unnumbered*, the Inverse ARP choice is blanked out. This option is provided to interoperate with other vendors that treat Frame Relay as a non-broadcast multi-access (NBMA) interface.

Routers that treat an interface configured for Frame Relay as an NBMA interface can use Inverse ARP to learn the IP address of the remote router associated with a DLCI. These routers usually have the ability to use static mapping instead of Inverse ARP. Enable this option if the remote router requires Inverse ARP. NBMA with Inverse ARP is the default on Cisco routers.

Inverse ARP is not needed by the Routermate Router since it treats Frame Relay as a series of point-to-point connections.

Enabled - the router will send and respond to Inverse ARP requests as defined in RFC 1293.

Disabled - the unit ignores Inverse ARP requests and does not send Inverse ARP requests.

Default: *Disabled*

5.5.1.3 IP Filters

Figure 5-13 illustrates the Port IP Filters screen. In an IP environment, the IP Routing Information Protocol (RIP) exchanges routing information with other routers. IP filters can be used to reduce the amount of IP routing traffic on the WAN link, and to restrict access between certain networks. If IP Filters are enabled for a port, use this screen to enable or disable specific types of filters for that port.

The screen is the same for LAN and WAN ports.

To access the Filter Tables listed on the screen, position the cursor on the desired selection and press **[CR]**.

Announce Static Routes - enable/disable port's ability to advertise user-defined IP routes out the specified port.

Enabled - port advertises IP static routes.

Disabled - port does not advertise IP static routes.

Default: *Enabled*

Announce Default Route - enable/disable port's ability to advertise the default route out the specified port.

Enabled - port advertises the default route.

Disabled - port does not advertise the default route.

Default: *Enabled*

Learn Default Route - enable/disable port's ability to learn the default route on the specified port.

Enabled - port learns the default route.

Disabled - prevents the default route from being learned on this port.

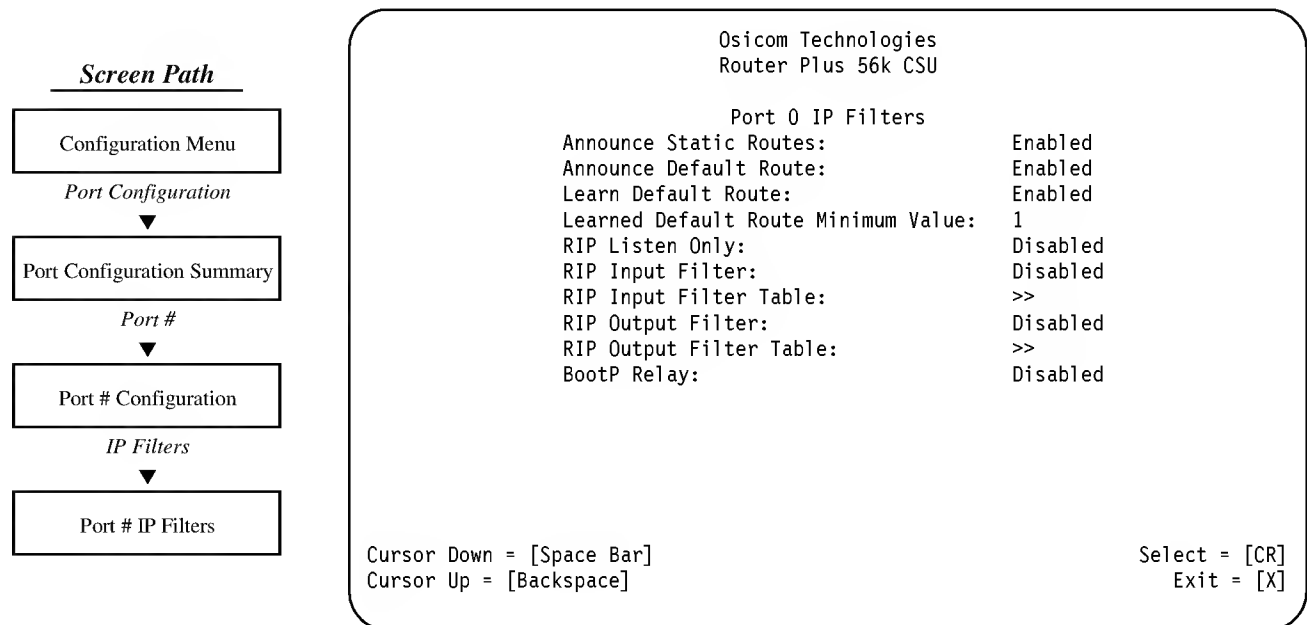


Figure 5-13. IP Filters

Learned Default Route Minimum Value - allows the user to set a minimum default route metric. When a default route is learned, the metric placed in the routing table will be the larger of the learned metric and the Learned Default Route Minimum Value.

Valid range: 1-14.

Default: 1

RIP Listen Only - determines port's handling of RIP messages.

Enabled - port learns routes, but routes are not advertised on this port.

Disabled - routes are learned and advertised on this port.

Default: *Disabled*

RIP Input Filter - filters received RIP messages.

Negative - RIP entries that match a filter are discarded; all others are passed.

Disabled - RIP entries are not filtered.

Default: *Disabled*

RIP Output Filter - filters transmitted RIP messages.

Positive - RIP entries that match a filter are passed; all others are discarded.

Disabled - RIP entries are not filtered.

Default: *Disabled*

BootP Relay - the router listens for BootP request on UDP port number 67 on ports with the *BootP Relay* option enabled. Any BootP request received from the client will be forwarded out all ports with the *BootP Relay* option enabled except for the port the BootP request was received on. For a client to access a remote BootP server, the *BootP Relay* option must be enabled on all of the ports in the path between the client and the server including the ports that the client and server are attached to. See RFC951 and RFC1542 for more details.

Enabled - BootP Relay process allowed.

Disabled - BootP Relay process prevented.

5.5.1.3.1 IP RIP Input/Output Filters

The port IP RIP Input and Output Filter Table screens are identical (except for the screen name) as shown in Figure 5-14. IP addresses configured for each table are handled differently, as described below:

The **Input Filter Table** is also called the *Reject List*. If RIP input filters are enabled, use this screen to specify the IP address of networks that are not allowed to be learned on this port from the routing update packet.

The **Output Filter Table** is also called the *Advertise List*. If RIP output filters are enabled, use this screen to specify the IP address of networks that are allowed to be advertised over this port. Only the addresses listed in the table are advertised over this port.

Address range: 0.0.0.0 to 255.255.255.255

Default: *Blank*

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**.
2. Edit/configure the address. Press **[CR]** again to de-select.

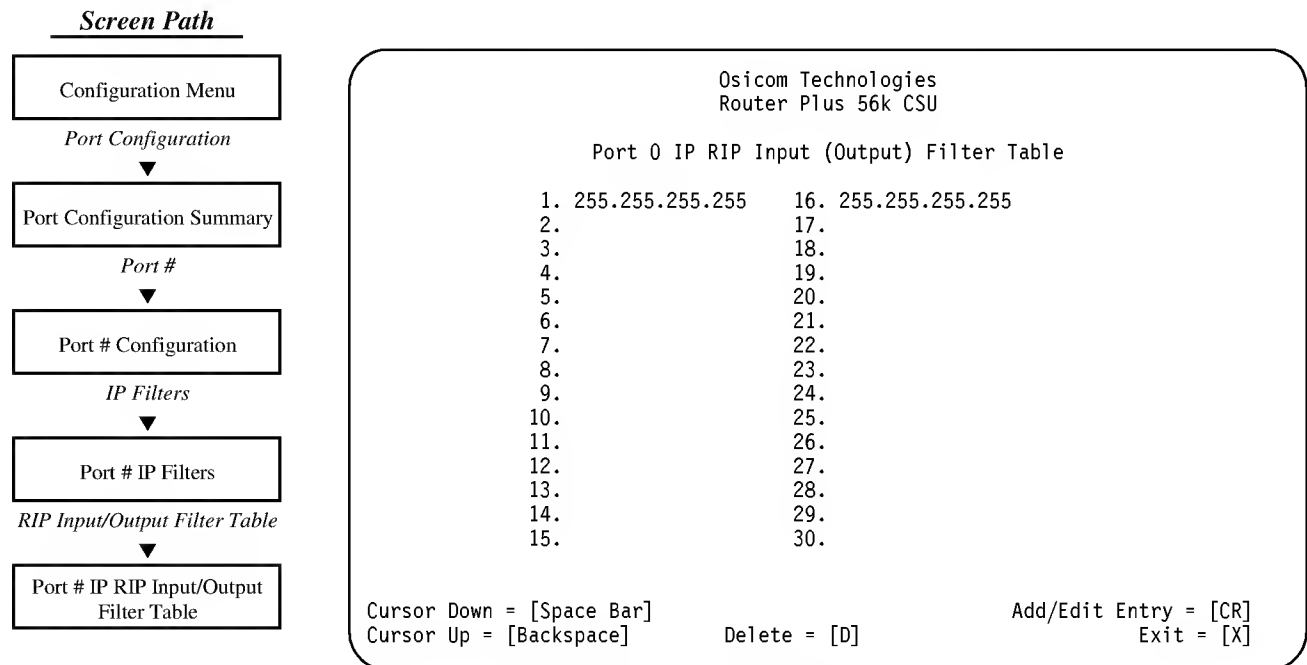


Figure 5-14. Port IP RIP Input (Output) Filter Table

5.5.1.4 IPX Routing Options

Access the Port IPX Routing Options screen to configure IPX routing options for the LAN and WAN interfaces. IPX routing options for ports mapped to the LAN and WAN interfaces are identical except for the parameters noted.

IPX Network Number - the IPX network number for the this port. Each port must have a unique network number. When the Mode is changed from Unnumbered to Numbered the default value of all zeros is displayed. The user is not allowed to save changes with a duplicate or all zeros number displayed. An "Invalid Network Number" message is displayed if Yes is entered at the *save configuration* prompt.

Valid input: 32-bit hex range *00000001* to *FFFFFFFE*. All zeros indicate no address defined.

Default: *00000000*

Frame Type (LAN only) - the frame type to be used for IPX transmissions out the LAN interface. Select the option to match the frame type that is used by the Novell servers and clients on the LAN you are connected to. Novell servers and clients support four different types of ethernet encapsulation (frame type). The default value that a server and client use is different for various software revisions. Selecting the wrong frame type is a common IPX configuration error and will prevent the Routermate Plus from communicating with Novell servers and clients. The Routermate Plus will only route the frame type selected. All other frame types will be bridged (if bridging is enabled).

Valid input: *Type II*, *802.3 (RAW)*, *802.2 (LLC)*, or *SNAP*

Default: *802.2*

Mode (WAN only) - set the operating mode for this port.

Numbered - an IPX network number is assigned to this port.

Unnumbered - an IPX Network Number is not assigned to this port; the IPX Network Number option is blanked out.

Unnumbered mode decreases the size of the routing

table since no direct routes are created for the WAN ports. This reduces the amount of memory required to hold the routing table and also decreases the amount of bandwidth used to send routing updates.

IPXWAN (WAN only) - a protocol developed by Novell and specified in RFC1634. The purpose of IPXWAN is to provide a common way of exchanging router to router information across different type of wide area links. RFC1634 describes how Novell IPX operates over various WAN media using the IPXWAN protocol.

Support for IPXWAN is only provided to allow the router to be compatible with Novell routers. It is not required to route IPX and should be disabled unless it is required.

NOTE

IPXWAN must be set to the same value on both ends of a connection. If it is not set to the same value, then the router will not be able to communicate across the link.

Default: *Disabled*

Transport Time - sets the weight (in time ticks) associated with this port. This determines the delay entered in the IPX Routing Table for the direct route associated with this port. The Transport Time value is added to the value shown in the IPX Routing Table for each route advertised on this port. Set the Transport Time to the estimated amount of time to send a 576-byte packet on this port. For interfaces with more than 1Mbps of bandwidth, set the Transport Time to 1 tick.

There are 18.21 time ticks in a second, so a time tick equals approximately 1/18 second or 55 ms.

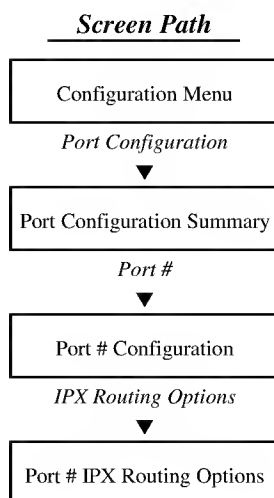
Valid input: *1 to 255 ticks*

Default: *1 tick*

Periodic RIP Timer - the time interval between periodic IPX RIP broadcasts transmitted out the specified virtual IPX port.

Valid input: *30 to 999 seconds*

Default: *60 s*



```

Osicom Technologies
Router Plus 56k CSU

Port 0 IPX Routing Options

IPX Network Number: 00000000
Frame Type: 802.2
Transport Time: 1 ticks
Periodic RIP Timer: 60 s
RIP Age Timer: 180 s
Periodic SAP Timer: 60 s
SAP Age Timer: 180 s

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Edit Field = [CR]
Exit = [X]
  
```

Figure 5-15. Port 0 IPX Routing Options (LAN)

```

Osicom Technologies
Router Plus 56k CSU

Port 1 IPX Routing Options

Mode: Unnumbered
IPX Network Number:
IPXWAN: Disabled
Transport Time: 5 ticks
Periodic RIP Timer: 60 s
RIP Age Timer: 180 s
Periodic SAP Timer: 60 s
SAP Age Timer: 180 s
Inverse ARP:

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Edit Field = [CR]
Exit = [X]
  
```

Figure 5-16. Port 1 IPX Routing Options (WAN)

RIP Age Timer - the maximum time between RIP update messages before a route that was learned (i.e., that was added to the IPX Routing Table as the result of an IPX RIP update message) is removed from the IPX routing table. If an update message is received for an address, the internal aging count reverts to zero. If no update message is received by the time configured for the RIP Age Timer, the route is removed from the IPX Routing Table.

Valid input: 30 to 9999 seconds

Default: 180 s

Periodic SAP Timer - the time interval between periodic IPX SAP broadcasts transmitted out the specified virtual IPX port.

Valid input: 30 to 999 seconds

Default: 60 s

SAP Age Timer - the maximum time between SAP update messages before the server that was learned (i.e., that was added to the IPX Services Table as the result of an IPX SAP update message) is removed from the IPX Services Table. If an update message is received for a service, the aging count for that server reverts to zero. If no update message is received by the time configured for this timer, the server is removed from the IPX Services Table.

Valid input: 30 to 9999 seconds

Default: 180 s

Inverse ARP (WAN only) - applies only if the Protocol is set to Frame Relay (see WAN Configuration screen (Section 5.4.2, page 5-9) and the Mode is *Numbered*. When the Mode is *Unnumbered*, the Inverse ARP choice is blanked out. This option is provided to interoperate with other vendors that treat Frame Relay as a non-broadcast multi-access (NBMA) interface.

Routers that treat an interface configured for Frame Relay as an NBMA interface can use Inverse ARP to learn the IPX address of the remote router associated with a DLCI. These routers usually have the ability to use static mapping instead of Inverse ARP. Enable this option if the remote router requires Inverse ARP. NBMA with Inverse ARP is the default on Cisco routers.

Inverse ARP is not needed by the Routermate Router since it treats Frame Relay as a series of point-to-point connections.

Enabled - the router will send and respond to Inverse ARP requests as defined in RFC 1293.

Disabled - the unit ignores Inverse ARP requests and does not send Inverse ARP requests.

Default: *Disabled*

5.5.1.5 IPX Filters

Access the Port IPX Filters screens to configure IPX filters, and to access configuration screens for enabled filters. Use IPX filters to reduce the amount of IPX routing traffic on the LAN or WAN link, and to restrict access between certain networks.

To display the filter tables listed in the screen, move the cursor to the desired selection and press **[CR]**.

Diagnostic Packets (LAN only) - a filter for diagnostic packets on the specified virtual IPX port.

Forward - the port will pass the diagnostic packet.

Filter - packets with a destination socket number of 456 are filtered at the receiving port.

Default: *Forward*

Serialization Packets (LAN only) - a filter for Novell serialization security packets on the specified virtual IPX port. Novell Netware File Servers broadcast security packets that contain serialization information regarding the license of the file server executable. Serialization packets consume valuable bandwidth over a low-speed serial WAN link. Disabling the broadcast of serialization packets reduces WAN traffic. Disabling serialization packets is not intended to interfere with copyright protection mechanisms.

Forward - the port will pass serialization packets.

Filter - packets with a destination socket number of 457 are filtered at the receiving port.

Default: *Forward*

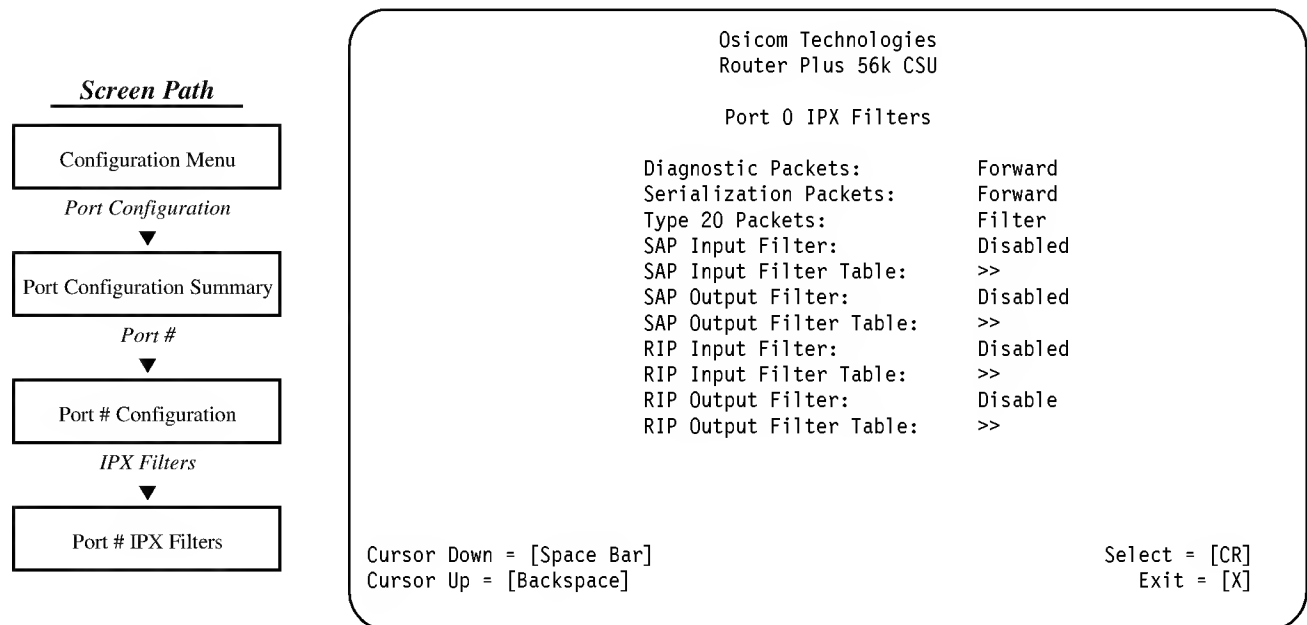


Figure 5-17. Port 0 IPX Filters (LAN)

Type 20 Packets - these packets are used to propagate broadcast messages using different protocol through the IPX network. The most common use is NetBIOS encapsulated in IPX.

Broadcast - Type 20 packets received on this port will be broadcast out all other ports with IPX Routing enabled and the Type 20 Packets option set to *Broadcast*.

Filter - disables the processing of Type 20 packets.

Default: *Filter*

Watchdog Packets (WAN only) - the method of Novell File Server "Keep-Alive" Watchdog Spoofing. When a Netware workstation logs into a Novell server, the server issues periodic Keep-Alive messages to the client in order to determine if the workstation is active. The Keep-Alives can consume considerable bandwidth on low-speed serial links. Watchdog packets received on the LAN that are to be forwarded across a WAN port with watchdog spoofing enabled are spoofed.

Spoofed - this option is enabled.

Forward - watchdog packets are not spoofed.

Default: *Forward*

SAP and RIP Input Filters - applied to RIP and SAP update messages received by a port. The filters control what is entered in the IPX SAP and RIP tables.

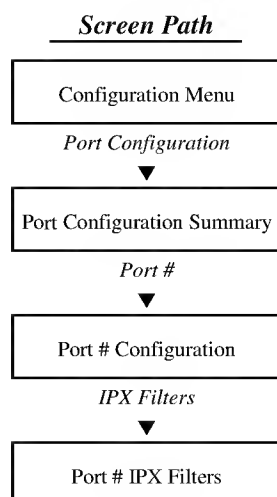
SAP and RIP Output Filters - applied to RIP and SAP update messages transmitted by a port. The filters control what is advertised on the specified port.

Positive Filter - SAP/RIP entries that match a filter entry are passed; all others are discarded.

Negative Filter - SAP/RIP entries that match a filter entry are discarded; all others are passed.

Disabled - the filter table is not used.

Default: *Disabled*



```

Osicom Technologies
Router Plus 56k CSU

Port 1 IPX Filters

Type 20 Packets:      Filter
Watchdog Packets:    Forward
SAP Input Filter:     Disabled
SAP Input Filter Table:  >>
SAP Output Filter:    Disabled
SAP Output Filter Table: >>
RIP Input Filter:     Disabled
RIP Input Filter Table: >>
RIP Output Filter:    Disabled
RIP Output Filter Table: >>

Cursor Down = [Space Bar]      Select = [CR]
Cursor Up   = [Backspace]     Exit   = [X]
  
```

Figure 5-18. Port 1 IPX Filters (WAN)

5.5.1.5.1 IPX SAP Input/Output Filters

Both the Port IPX SAP Input Filter Table and the Port IPX SAP Output Filter Table are shown in Figure 5-19, page 5-31. The two tables are identical in appearance. Input filters are applied to SAP or RIP entries received by a port; they control what is entered in the local routers SAP or RIP tables. Output filters are applied to SAP or RIP entries transmitted by a port; they control what is advertised by the local router.

The IPX Service Advertising Protocol (SAP) lets IPX advertise Novell IPX services offered by such devices as file servers (file transfer), printer servers (print service), and gateways (protocol conversion). SAP filters can be used to filter SAP update packets.

To access the tables, select either **SAP Input Filter Table** or **SAP Output Filter Table** at the Port IPX Filters screen.

The maximum number of entries for each table is 28. If more than 14 entries are configured, press **[+]** or **[-]** to toggle between pages 1 and 2.

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**; the IPX SAP Input (or Output) Filter screen (Figure 5-22) is displayed.
2. At the Filter screen, move the cursor to the desired field and press **[CR]** to select the field.
3. Configure each parameter as required.
4. Press **[X]** to return to the Filter Table.

To delete an entry, position the cursor on it and press **[D]**.

All filter options are taken into account when filtering. The user can configure any combination of the filter options or all of the options.

Setting the Network Address, Filter Mask, Node Address, Server Type, and Server Name to their default value indicates no table entry. Setting any one of these options to a non-default value causes an entry in the filter table.

Saving an entry with all default values does not cause an entry to be placed in the table.

Don't care fields can be configured in an entry, as follows:

- Saving an entry with a network address of all zeroes and a filter mask of FFFFFFFF causes these fields to be blank in the SAP Filter Table, and indicates that the network address is not tested by a filter.
- Saving an entry with all zeroes for the service type or node address causes these fields to be blank in the SAP Filter Table, and these fields are not tested by a filter.
- If the server name is blank, the server name is not tested by a filter.

Filter State - enable/disable the filter.

Default: *Enabled*

Network Address - IPX network number for the router's interface (must match the network number of the Novell device's interface to which it is attached).

Valid input: 32-bit hex range 00000000 to FFFFFFFF.

Default: 00000000; indicates no network address configured.

Filter Mask - used in a logical 'AND' with the network address to determine which part of the network address should be considered. For example, configuring a network address of ABCD0000 and a filter mask of FFFF0000 causes the filter to be applied to addresses ABCD0000 through ABCDFFFF. Configuring a network address of 00000000 and a filter mask of FFFF0000 causes the filter to be applied to addresses 00000001 through 0000FFFF.

Valid input: 32-bit hex range 00000001 to FFFFFFFF

Default: FFFFFFFF

Node Address - the end-station node address assigned to the router. The node address is assigned the same value as the MAC address. This address must match one of the addresses assigned to the router interfaces. When a node address is specified, the filter is applied against the specified network address, or against all networks if the network address is set to all zeros.

Valid input: 48-bit hex range 000000000000 to FFFFFFFF

Default: 000000000000; no node address configured.

Server Type - the type of service provided by the server.

Table 5-1 lists several commonly-used service types.

Valid input: 16-bit hex range 0000 to FFFF

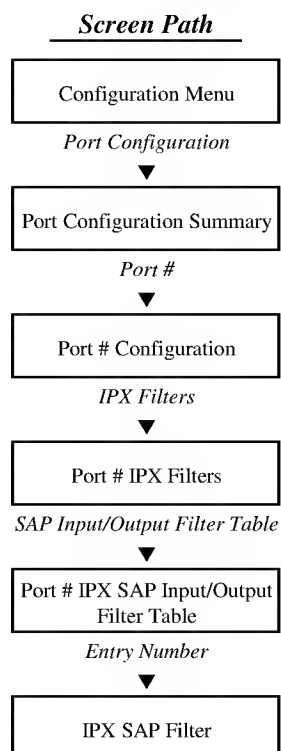
Default: 0000; no server type configured

Server Name - the text name for the server that is distributed to other IPX services via SAP messages.

Valid input: Up to 48 alphanumeric characters. A shortened form of the server name is displayed on the SAP Filter Table.

Default: *Blank*

Table 5-1. Selected IPX Services	
SERVICE	SERVER TYPE
User	1
User Group	2
Print Queue	3
File Server	4
Job Server	5
Gateway	6
Print Server	7
Archive Queue	8
Archive Server	9
Job Queue	A
Administration	B
Remote Bridge Server 2	24
Bridge Server	26
TCP/IP Gateway	27
Archive Server SAP	2e
Advertising Print Server	47
Print Queue User	53
HP Laserjet	30c
Wildcard	FFFF



Osicom Technologies
Router Plus 56k CSU

Port 1 IPX SAP Input (Output) Filter Table - Page 1

Filter State	Network Address	Filter Mask	Node Address	Server Type	Server Name
1. Enabled	E0100000	FFFFFFF	08000E000123	A027	Server 1
2. Enabled	00000000	FFFF0000		1027	Server 2
3. Disabled	10100000	FFFFFFF	08000E000101	2027	12345678901234567890
4. Enabled	E0100000	FFFFFFF		3000	
5. Enabled	20100000	FFFFFFF			
6. Enabled				1027	Server 3
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Cursor Down = [Space Bar] Delete = [D] Select Menu = [CR]
 Cursor Up = [Backspace] Page = [+] [-] Exit = [X]

Figure 5-19. Port 1 IPX SAP Input (Output) Filter Table

Osicom Technologies
Router Plus 56k CSU

Port 1 IPX SAP Input (Output) Filter

Filter State:	Enabled
Network Address:	00000000
Filter Mask:	FFFFFFF
Node Address:	000000000000
Server Type:	0000
Server Name:	1234567890123456789012345678901234567890123456789012345678

Cursor Down = [Space Bar] Select = [CR]
 Cursor Up = [Backspace] Exit = [X]

Figure 5-20. Port 1 IPX SAP Input (Output) Filter

5.5.1.5.2 IPX RIP Input/Output Filters

Figure 5-21 illustrates the filter table for both IPX RIP input and output filters. The screens for input and output filters are the same except for the screen name.

The configuration and operation of the IPX RIP Filters is similar to the IPX SAP Filters described in the previous section except the fields that can be filtered are different.

Routers in an IPX environment use the IPX Routing Information Protocol (RIP) to exchange routing information. IPX RIP is different from IP RIP, although the purposes of both are similar.

To access the tables, select **RIP Input Filter Table** or **RIP Output Filter Table** at the Port IPX Filters screen.

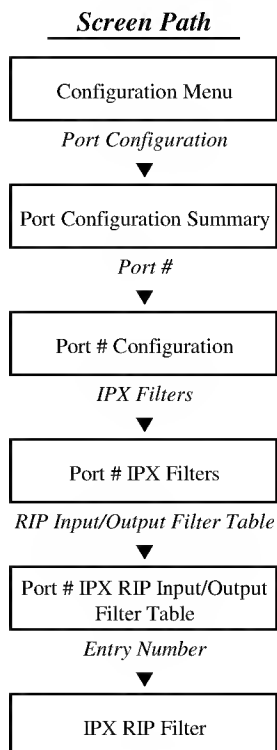
The maximum number of entries for each table is 30. If more than 15 entries are configured, press **[+]** or **[-]** to toggle between pages 1 and 2.

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**; the IPX RIP Input (or Output) Filter screen (Figure 5-22) is displayed.
2. At the Filter screen, move the cursor to the desired field and press **[CR]** to select the field.
3. Configure each parameter as required.
4. Press **[X]** to return to the Filter Table.

To delete an entry, position the cursor on it and press **[D]**.

Saving an entry with all default values does not cause an entry to be placed in the table.



Osicom Technologies Router Plus 56k CSU		
Port 1 IPX RIP Input (Output) Filter Table - Page 1		
Filter State	Network Address	Filter Mask
1. Enabled	E0100000	FFFFFFFF
2. Enabled	00000000	FFFFFFFF
3. Disabled	10100000	FFFFFFFF
4. Enabled	E0100000	FFFFFFFF
5. Enabled	20100000	FFFFFFFF
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
Cursor Down = [Space Bar] Delete = [D] Select Menu = [CR] Cursor Up = [Backspace] Page = [+] [-] Exit = [X]		

Figure 5-21. Port 1 IPX RIP Input (Output) Filter Table

Osicom Technologies Router Plus 56k CSU	
Port 1 IPX RIP Input (Output) Filter	
Filter State:	Enabled
Network Address:	00000000
Filter Mask:	FFFFFFFF
Cursor Down = [Space Bar] Select = [CR] Cursor Up = [Backspace] Exit = [X]	

Figure 5-22. Port 1 IPX RIP Input (Output) Filter

5.5.1.6 Bridging Options

Access the Port Bridging Options screen (Figure 5-23) to configure bridging options. Screens for the LAN and WAN interfaces are identical. .

Select **Transmit Filter Table** to display configured transmit filters for this port. See the following section.

Unicast Frame Flooding - enable/disable flooding of unicast frames on the port.

Enabled - unicast frames with an unknown destination address can be flooded on this port.

Disabled - no flooding will be done on this port; unicast frames with an unknown destination will not be transmitted .

Default: *Enabled*

Transmit Multicast - enable/disable transmission of all multicast frames on this port.

Enabled - transmits multicast frames destined for this port.

Disabled - discards multicast frames destined for this port.

Default: *Enabled*

Transmit Broadcast - enable/disable transmission of all broadcast frames on this port.

Enabled - transmits broadcast frames on this port.

Disabled - discards broadcast frames on this port.

Default: *Enabled*

Transmit Filter - determines how the entries in the Transmit Filters Table will be used.

Positive - frames which match at least one entry in the Transmit Filters Table will be forwarded; the rest are discarded.

Negative - frames which match at least one entry in the Transmit Filters Table will be discarded; the rest are forwarded.

Disabled - filters are not applied, no frames will be filtered based on the contents of the Transmit Filters Table.

Default: *Disabled*

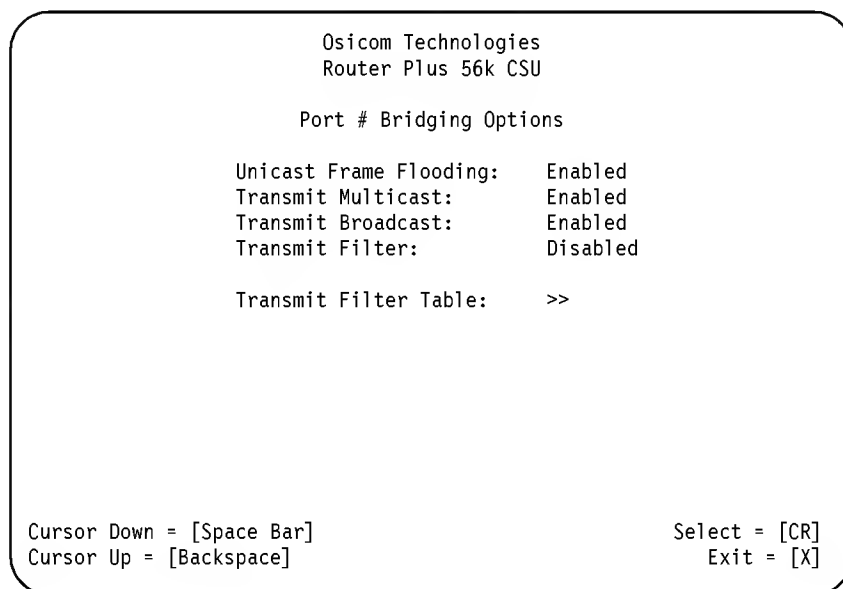
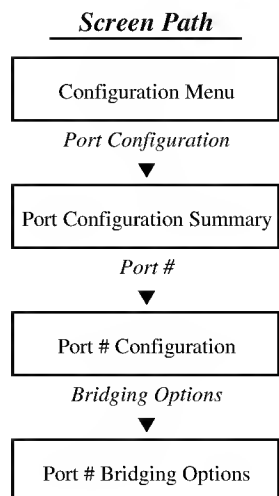


Figure 5-23. Bridging Options

5.5.1.6.1 Transmit Filters

Figure 5-24 illustrates the Transmit Filter Table. This screen displays up to five transmit filters for each port. The default configuration is for no filters to be configured.

Transmit filters typically are applied to the *Type* field in the Ethernet frame to filter specific types of Ethernet frames.

These filters are applied just before the frame is transmitted to the destination port, after address learning and bridging. This lets the filter be port specific.

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**; the port's Transmit Filter screen (Figure 5-25) is displayed.
2. At the Transmit Filter screen, configure each parameter as required.
3. Press **[X]** to return to the Transmit Filter Table.

If a blank entry is selected in the Transmit Filter Table, and *No* is selected in response to the confirmation prompt, the entry remains blank and no entry is added to the Transmit Filter Table.

To delete an entry, move the cursor to the entry and type **[D]**.

Offset - the relative location in the frame of the two bytes to be compared with the *Type Value*. An offset of 0 would compare the filter's *Type Value* against the first two bytes of the destination address in the ethernet MAC header.

For example, to apply the filter to the bytes in the Ethernet frame that provide the *Type* code, set the value to 12. The filter will skip the 12 bytes (0 - 5 and 6 - 11) that contain the destination and source addresses in the MAC header before applying the filter). See **Type Value**, following.

Valid range: 0 - 1516

Default: 12

Type Value - the type of Ethernet frame to be filtered. This value is compared to the transmitted frame at the location in the frame specified by the offset value.

Specific types of Ethernet frames can be filtered. As shown below, the MAC header of an Ethernet frame contains a destination address and a source address, followed by a 2-byte *Type* value:

To filter a particular type of frame, enter the hexadecimal *Type* code (0000 through FFFF) for that frame type. Common Ethernet types are:

<i>Ethernet Type</i>	<i>Code</i>
XNS	0600
IP	0800
ARP	0806
DEC MOP Dump/Load	6001
DEC MOP Remote Console	6002
DECNET	6003
DEC LAT	6004
AppleTalk	809B

Filtering is applied to any frame with a *Type* code that matches the value specified in the **Type Value** field. A frame that matches will be either filtered or forwarded, depending upon the setting of the Transmit Filter (see previous section).

NOTE

If you configure the **Type Value** parameter, you must also configure the **Offset** parameter to specify the position of the value in the Ethernet frame.

Valid range: 0000 - FFFF

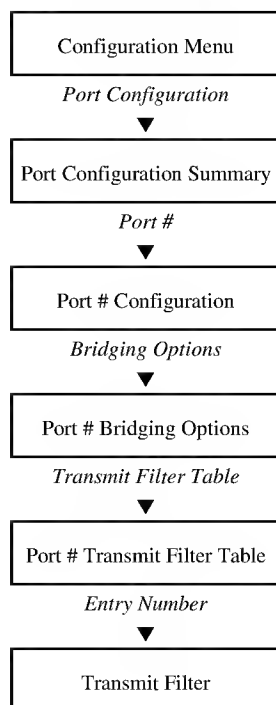
Default: 0000

A valid configuration is:

Offset = 0

Type Value = 0

Screen Path



```

Osicom Technologies
Router Plus 56k CSU

Port 0 Transmit Filter Table

      Offset      Type Value
1.      12      0x0800
2.
3.
4.
5.

Page Down = [+]
Page Up   = [-]

Delete = [D]

Select Menu = [CR]
Exit = [X]

```

Figure 5-24. Port Transmit Filter Table

```

Osicom Technologies
Router Plus 56k CSU

Port 0 Transmit Filter

Offset:      12
Type Value:  0000

Cursor Down = [Space Bar]
Cursor Up   = [Backspace]

Edit Field = [CR]
Exit       = [X]

```

Figure 5-25. Port Transmit Filter

5.5.1.7 Encryption Options (Frame Relay and PPP)

Use the Port Encryption Options screen to configure encryption options for the WAN interface. Encryption applies only if the router has the optional encryption hardware installed.

NOTES

Restricted Access - The Encryption Options screen is not available unless the user has entered the **Key Password** to access the management screens (see *Password* in Chapter 3). This applies to terminal or Telnet access.

To activate encryption options, Encryption must be *Enabled* on the Port Configuration screen (see Section 5.5.1, page 5-13).

The Routermate Plus can encrypt data using the Data Encryption Standard (DES) algorithm. The DES algorithm is implemented in optional hardware, and uses a 56-bit key to convert clear text into encrypted form. Although the DES technique is well known, it is very difficult to recover the original data without the key used to encrypt it. To recover the original data, the DES algorithm is run in reverse, using the original encryption key. The security of the data is based on secrecy of the key used in its encryption. It is important to minimize exposure of the encryption key, and to change it regularly.

Prior to transmission over Frame Relay, the router encrypts all but the first two bytes of each frame. On reception, the receiving router applies DES to recover the original frame contents. It is important that both ends of the PPP link (or PVC if Frame Relay) use the same DES key. When using Frame Relay, the LMI traffic is sent and received in the clear.

To enhance security of key distribution, the router uses the DES algorithm to encrypt and decrypt the keys themselves. The encryption keys can be entered in either a clear or encrypted form. The router keeps all keys in encrypted form and decrypts them only just prior to their use in encrypting or decrypting data frames. It is highly recommended that keys be managed only in their encrypted form. Use of the clear DES key is unnecessary.

To eliminate downtime experienced when changing encryption keys, the router provides a way to simultaneously update the keys in multiple routers. Keys

can be entered as Pending Keys and a Key Update Time can be set. When the Key Update Time arrives, all routers convert their Pending Keys into the active Current encryption keys. Synchronizing the clocks of the routers allows key changes to happen at the same time.

To configure DES encryption of a PPP link:

1. Log out, then log back into the terminal interface screens using the **Key Password** (default is **[CR]**).
2. If the time shown in the top right corner of the screen is not correct, go to the Unit screen (Chapter 8) and set it to the correct time.
3. Go to the Port Configuration screen (see page 5-15) and enable encryption.
4. On the Encryption Options screen (Figure 5-26), enter a DES key as a Pending, Encrypted key. Although the key seems to be known, it will be DES decrypted prior to use. Thus, the key which is ultimately used to encrypt and decrypt data is really unknown, and likely more random than the key which is entered.

NOTE

It is possible to directly change the Current Key, but as soon as this new Current Key is confirmed, the WAN link will not pass data traffic until the remote router's Current Key is set to the same value.

5. Exit these screens and confirm the changes.
6. Access the Encryption Global Configuration screen (page 5-51) and enter the Key Update Time, which is the time in the future at which the new (Pending) encryption key takes effect. Exit from the screen and confirm the change. The Key Update Time should now be displayed in the top left corner of the terminal display.
7. Prior to logging out, save the configuration, so that the key configuration will not be lost should a power interruption occur.
8. Perform the same steps (1..7) in the remote router(s). Be sure that the identical encryption key is entered. Also be sure that the Key Update Time is effectively the same for each router. To avoid time zone conflicts, it is good policy to set the clocks in all interconnected routers to a universal time, rather than use local time.

At the Key Update Time, the new keys will be implemented and the Key Update Time erased from the top left corner of the screen display. From that point, the data on the WAN interface will be secured by DES encryption.

Current Key - the DES encryption key which is currently in active use.

Pending Key - the DES encryption key which is pending, awaiting the next Key Update Time, at which time it will be copied into the Current Key field and become the active encryption key.

Encrypted Key - the encrypted form of the current or pending DES encryption key. This key is internally decrypted prior to its use to encrypt and decrypt frame data transmitted and received on the WAN interface. The intent is to enter and distribute all DES keys in their encrypted form.

Valid range: 00 00 00 00 00 00 00 00 to
FF FF FF FF FF FF FF FF

Default: 00 00 00 00 00 00 00 00
(disables encryption)

Clear Key - provides an alternate way to configure the current or pending DES encryption key. When entering this key, all zeros are displayed and it is immediately encrypted and displayed in the Encrypted Key field. It is normally unnecessary and undesirable to enter the encryption key in clear form.

Valid range: (DES) 00 00 00 00 00 00 00 00 to
FF FF FF FF FF FF FF FF (DES)

(E-DES) _0 00 _0 00 _0 00 _0 00 to
_F FF _F FF _F FF _F FF

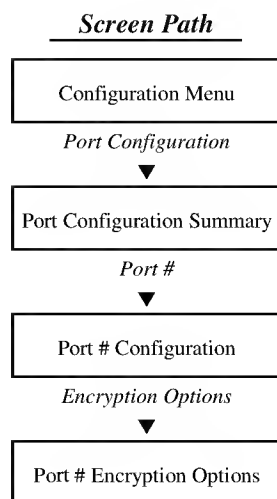
NOTE

In the E-DES (proprietary) version, the cursor skips over the underlined (blank) spaces because they are not configurable.

Default: 00 00 00 00 00 00 00 00
(disables encryption)

If entering keys in clear form, it is recommended to avoid these known weak keys:

00 00 00 00 00 00 00 00 (no key defined)
00 00 00 00 FF FF FF FF
FF FF FF FF 00 00 00 00
FF FF FF FF FF FF FF FF



12:00:00

Osicom Technologies
 Router Plus 56k CSU

Port 1 Encryption Options

	Clear Key	Encrypted Key
Current Key:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
Pending Key:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Cursor Down = [Space Bar]
 Cursor Up = [Backspace]

Edit Field = [CR]
 Exit = [X]

Figure 5-26. Encryption Options (Frame Relay and PPP)

5.6 Global Configuration

Use the Global Configuration screen (Figure 5-27) to access global configuration parameters for the router. Global parameters are not port-specific; they apply to all interfaces on the router.

NOTE

Encryption applies only if the router has the optional encryption daughter card installed.

For units that include the optional encryption feature, the Encryption Options screen cannot be accessed and encryption options cannot be configured unless the **Key Password** is used to access the management screens. This applies to terminal or Telnet access of the management screens.

See the following pages for details on each of the global configuration screens:

IP Global Configuration, page 5-40.

IPX Global Configuration, page 5-45.

Bridging Global Configuration, page 5-46.

PPP Global Configuration, page 5-50.

Encryption Global Configuration, page 5-51.

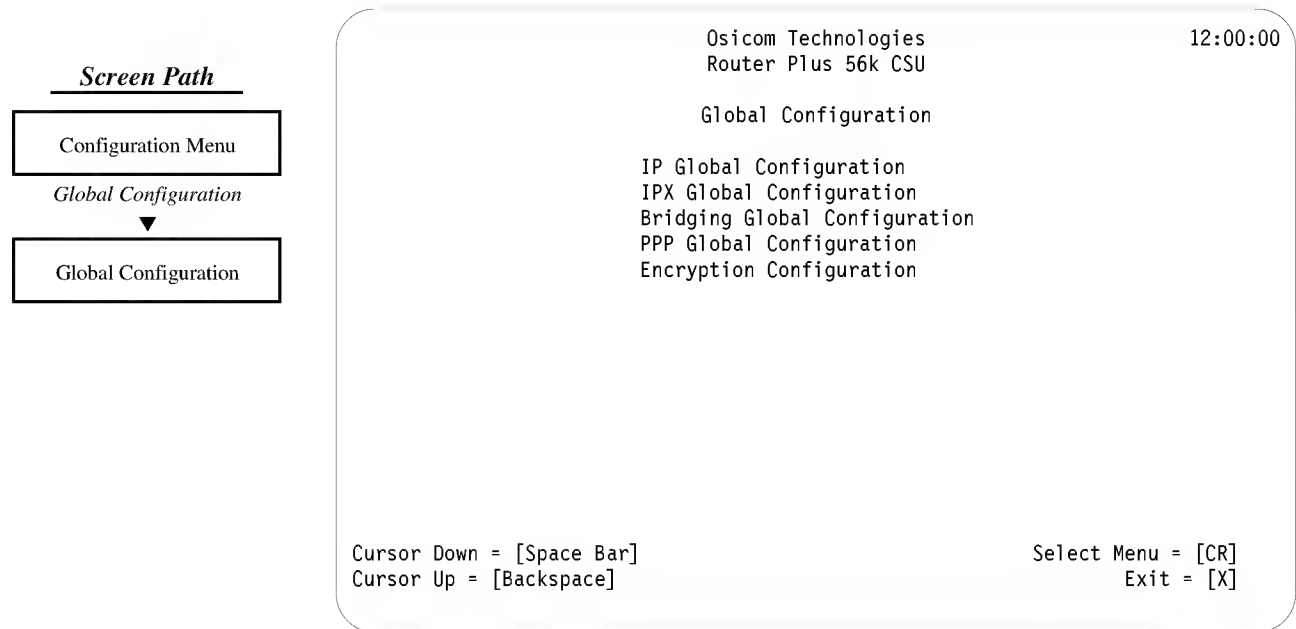


Figure 5-27. Global Configuration

5.6.1 IP Global Configuration

Access the IP Global Configuration screen to configure global IP options as shown in Figure 5-28.

Select the **Static Route Table** to configure static routes for routing. See IP Static Routes in next section.

Select the **RIP Neighbor List Table** to enter or edit IP addresses of directly-connected routers (any adjacent router) from which IP RIP update packets will be accepted. See IP RIP Neighbor List Table in Section 5.6.1.2, page 5-44.

Default Route Port - the default port for IP routing.

Enter the port number to which packets are to be forwarded when the destination address in the packet is unknown. When default routing is enabled, an entry with a destination of 0.0.0.0 is put in the routing table. This entry is advertised out all the other ports that have IP routing and RIP enabled (unless filtering is enabled). When set to port 0, the Default Route Address value is displayed. When set to a value other than port 0, the Default Route Address value is blanked out.

Valid input: *Disabled or range of configured ports*

Default: *Disabled*

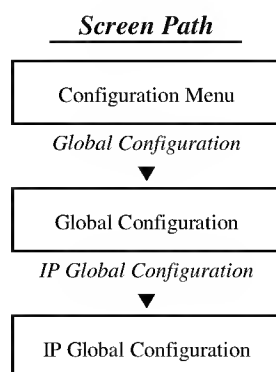
Default Route Address - enter the IP address of the router to which packets are to be forwarded when the destination address in the packet is unknown. The host portion of the address cannot be all zeros. If an incorrect address is entered, the "Invalid Address" message is displayed if Yes is entered at the save configuration prompt. The router automatically resolves the IP address to a port number via the IP Routing Table.

Default: *0.0.0.0* (disabled; no address defined)

Default Route Metric - sets the weight (number of hops) associated with the default route. This determines the number of hops to enter in the IP Routing Table for the default route (0.0.0.0).

Valid input: *1 to 15*

Default: *1*



```

Osicom Technologies
Router Plus 56k CSU

IP Global Configuration

Default Route Port:      Disabled
Default Route Address:
Default Route Metric:    1
Static Route Table:      >>
RIP Neighbor List:       Disabled
RIP Neighbor List Table: >>
BootP Seconds Threshold: 30
BootP Hops Threshold:    4
Subnet Zero:             Disabled

Cursor Down = [Space Bar]      Edit Field = [CR]
Cursor Up   = [Backspace]      Exit     = [X]
  
```

Figure 5-28. IP Global Configuration

RIP Neighbor List - enable/disable use of the RIP Neighbor List Table. RIP Neighbor List cannot be used on Unnumbered links.

Enabled - the RIP Neighbor List specifies the directly connected routers that routing update packets are accepted from.

Disabled - routing updates are accepted from all neighbors.

Default: *Disabled*

BootP Seconds Threshold - the BootP message contains a field that the booting machine fills in with the number of seconds since it began to boot. If the BootP Threshold Seconds filter is set, the router will not forward any BootP for a machine that booted more than x seconds ago. This is useful if a machine doesn't get a BootP reply, but keeps retrying for a long period of time.

Valid range: 1-300

Default: 30

BootP Hops Threshold - the BootP message has a field called Hops that is incremented by each router that forwards the message. The BootP Threshold Hops says to discard any BootP message whose Hops counter is greater than the configured value.

Valid range: 1-15

Default: 4

Subnet Zero - this option determines:

- If a subnet zero route will be learned.
- If the subnet portion of the **Address** can be set to zero on the IP Port Configuration screen.
- If the subnet portion of the **Destination** (address of target router or network) can be set to zero on the IP Static Route configuration screen.

Valid input: *Enabled or Disabled*

Default: *Disabled*

NOTE

Using Subnet Zero is discouraged because of the possibility that confusion could exist between a network route and a subnet route that have the same address. For example, if network 130.110.0.0 is subnetted as 255.255.255.0, the subnet zero route would be 130.110.0.0 which is the same as the network route.

5.6.1.1 IP Static Routes

The IP Static Route Table (Figure 5-29) lists static (user-defined) routes. Create a static route if the router cannot dynamically build a route to the destination (e.g., the route is to a router that does not implement RIP), or to reduce the amount of traffic used to exchange routing information. RIP announces static routes to other routers (unless filtering is enabled).

The maximum number of entries is 30. If more than 15 static routes are configured, use **[+]** and **[-]** to scroll between screens.

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**; the IP Static Route screen (Figure 5-30) is displayed.
2. At the IP Static Route screen, configure each parameter as required.
3. Press **[X]** to return to the Static Route Table.

Destination - the IP address for the target router or network. The host portion must be set to zero.

Default: *0.0.0.0*

Subnet Mask - if IP subnetting is used, identifies the parts of the IP address that are used for the network, subnetwork, and host numbers.

If IP subnetting is not used, ensure that this field is set to one of the following to match the network class of the configured IP address:

Network Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Default: *255.255.255.0*

Outgoing Port - identifies the port number for the static route.

Valid input: *Any configured port*

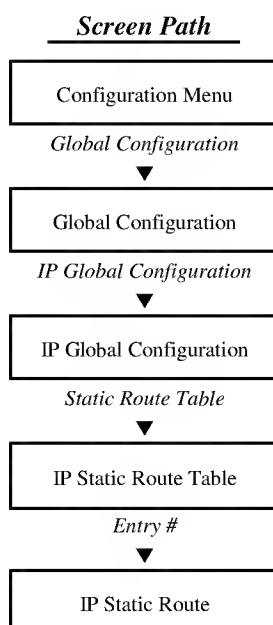
Next Hop - the IP address of the next router in the path toward the destination. The Next Hop address must be on a directly-connected network. The host portion cannot be set to all zeros. The Next Hop address is only displayed for a route that points towards the LAN (port 0); the Next Hop address is blanked out when the Outgoing Port is greater than 0.

Default: *0.0.0.0*. (not a valid host number)

Metric - the number of hops (intervening routers) between the source network and the destination network.

Valid input: *1 to 15*

Default: *1*



Osicom Technologies
Router Plus 56k CSU

IP Static Route Table - Page 1

	Destination	Subnet Mask	Port	Next Hop	Metric
1.	128.000.0.0	255.255.0.0	0	118.0.0.12	2
2.	129.102.0.0	255.255.0.0	0	118.0.0.12	4
3.	139.102.0.0	255.255.0.0	0	118.0.0.12	5
4.	149.102.0.0	255.255.0.0	0	118.0.0.12	15
5.	159.102.0.0	255.255.0.0	0	118.0.0.12	4
6.	169.102.0.0	255.255.0.0	0	118.0.0.12	9
7.	105.0.0.0	255.0.0.0	1	0.0.0.0	2
8.	108.0.0.0	255.0.0.0	1	0.0.0.0	2
9.					
10.					
11.					
12.					
13.					
14.					
15.					

Cursor Down = [Space Bar] Delete = [D] Select Menu = [CR]
 Cursor Up = [Backspace] Page = [+] [-] Exit = [X]

Figure 5-29. IP Static Route Table

Osicom Technologies
Router Plus 56k CSU

IP Static Route

Destination:	0.0.0.0
Subnet Mask:	0.0.0.0
Outgoing Port:	0
Next Hop:	0.0.0.0
Metric:	1

Cursor Down = [Space Bar] Edit Field = [CR]
 Cursor Up = [Backspace] Exit = [X]

Figure 5-30. IP Static Route

5.6.1.2 IP RIP Neighbor List Table

Access the IP RIP Neighbor List Table to enter or edit IP addresses of directly-connected routers (any adjacent router) from which IP RIP update packets will be accepted.

Press **[CR]** to edit an address.

Valid range: 0.0.0.0 to 255.255.255.255

Default: 0.0.0.0

To delete an address, position the cursor on that entry and press **[D]**; the default address (0.0.0.0) is displayed.

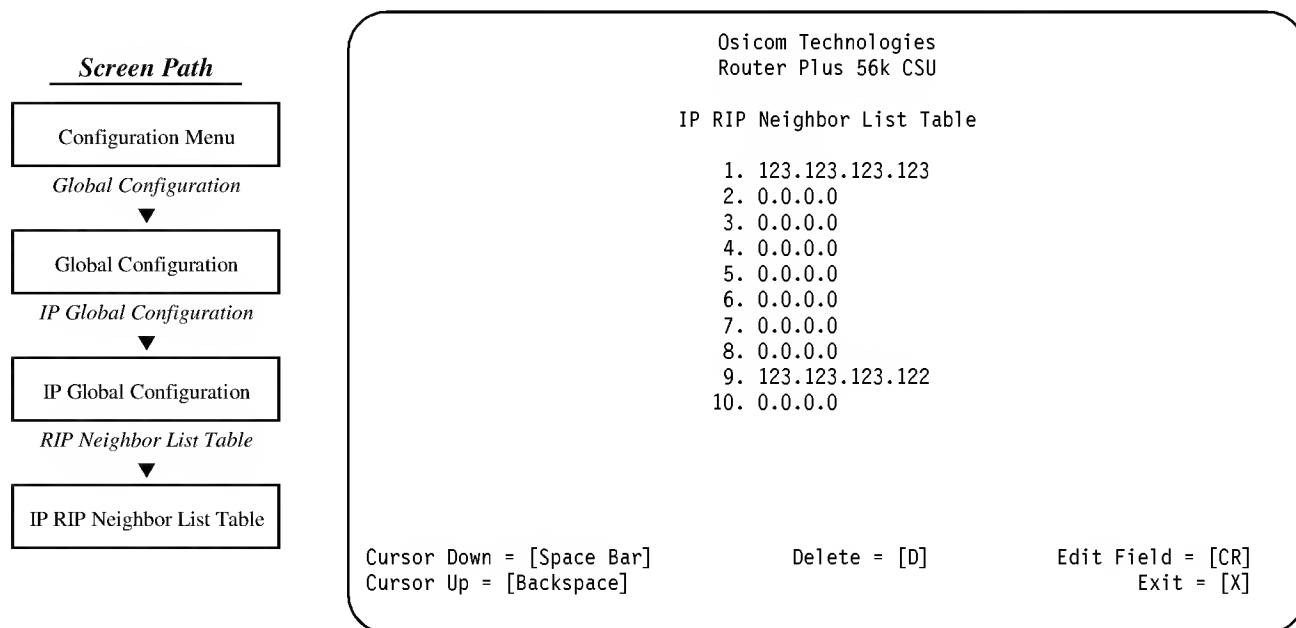


Figure 5-31. IP RIP Neighbor List Table (LAN)

5.6.2 IPX Global Configuration

Access the IPX Global Configuration screen (Figure 5-32) to configure global IPX options.

Internal Network Number - only used during IPXWAN initial negotiation to determine master slave roles. The router with the higher Internal Network Number is the master. IPXWAN is described in RFC1634.

Valid input: 32-bit hex range 00000000 to FFFFFFFF

Default: the value equal to the last 32 bits of the LAN interface's MAC address .

Gap Time - the minimum delay, in units of 55 milliseconds, between successive RIP or SAP messages. This option is provided because older Novell Servers may have a problem processing a series of RIP or SAP messages if the inter packet gap is not sufficient.

Valid input: 1 to 255 ticks (1 tick is 55 milliseconds).

Default: 2 ticks

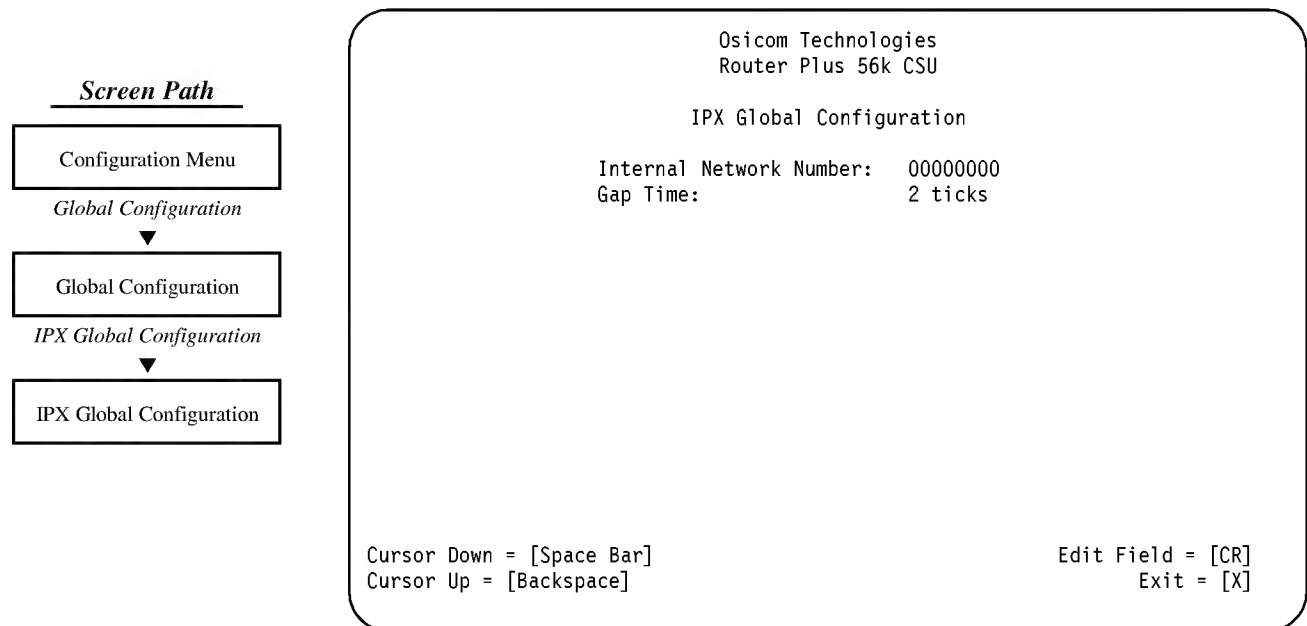


Figure 5-32. IPX Global Configuration

5.6.3 Bridging Global Configuration

Access the Bridging Global Configuration screen to configure global bridging options (Figure 5-33).

View the **Static Address Table** in the following section.

The **Address Learning** and **Forwarding Mode** options determine the default bridging action as follows. Entries in the Static Address Table cause the opposite action of the default action.

Configuration	Default Action
Address Learning: Enabled	Permit All
Forwarding Mode: Normal	
Address Learning: Disabled	Deny All
Forwarding Mode: NA	
Address Learning: Enabled	Deny All
Forwarding Mode: Restricted	

Address Learning - enables/disables address learning.

Enabled - the unit automatically learns source addresses. Frames with an unknown destination are broadcast.

Specifically, when an Ethernet frame is received and address learning is enabled, the unit looks in its address table for the received frame's destination address. If the destination address is located, the frame is forwarded. If the destination address is not located, then the frame is broadcast.

Disabled - frames will be forwarded only between statically entered addresses. Frames destined for addresses which are not in the address table will be discarded. Broadcast and Multicast frames from an unknown source are still flooded. Flooding broadcast frames from an unknown source is required for ARP to work across the bridge.

Default: *Enabled*

Forwarding Mode - used in conjunction with the Static Address Table (when address learning is enabled) to control which devices can communicate, as follows:

Normal - any device can communicate with any other device since address learning is enabled. A specific device can be prevented from communicating by adding the device's MAC Address to the Static Address Table and setting **Action** to *Filter* for that address; the bridge will not forward frames from or to this address.

Restricted - the bridge only forwards frames which are either sourced or destined to a static address table entry. Learning is not affected, so a frame transmitted from a statically-entered source address to an unknown destination will be flooded. Frames are not forwarded between two learned addresses. When forwarding is restricted, broadcasts (not multicasts) will be flooded either if the source address is known or the broadcast is from the WAN. Flooding broadcast from an unknown source is required for ARP to work across the bridge.

Default: *Normal*

WAN to WAN Forwarding - enables/disables bridging of frames between two wide area networks.

Enabled - frames received from a WAN port can be broadcast or flooded to the other WAN ports.

Disabled - frames received from a WAN port are not broadcast or flooded to another WAN port.

Default: *Enabled*

Address Aging Time - a process for determining how long an address which has not been used will remain in the address table. The time entered here is the maximum time that an automatically learned address can remain inactive before it is deleted.

The bridge can accommodate 2047 addresses. If the network is small and it is unlikely that the maximum number of addresses will be learned, set the aging time to a high number (31 days is the maximum). If the network is large, decrease the aging time so inactive Ethernet addresses are deleted, making more room for new addresses.

Decrease the aging time if the Ethernet devices are frequently moved between LANs. This lets the address be aged out and relearned at the new location.

If the aging time is set too low, the bridge might need to relearn addresses frequently, which can affect performance.

When editing the time, use two digits each for days, hours, and minutes. The colons (:) do not have to be typed between numbers.

Valid Range: 0-32 days:0-23 hours:0-59 minutes

Default: 00:01:00 (1 hour)

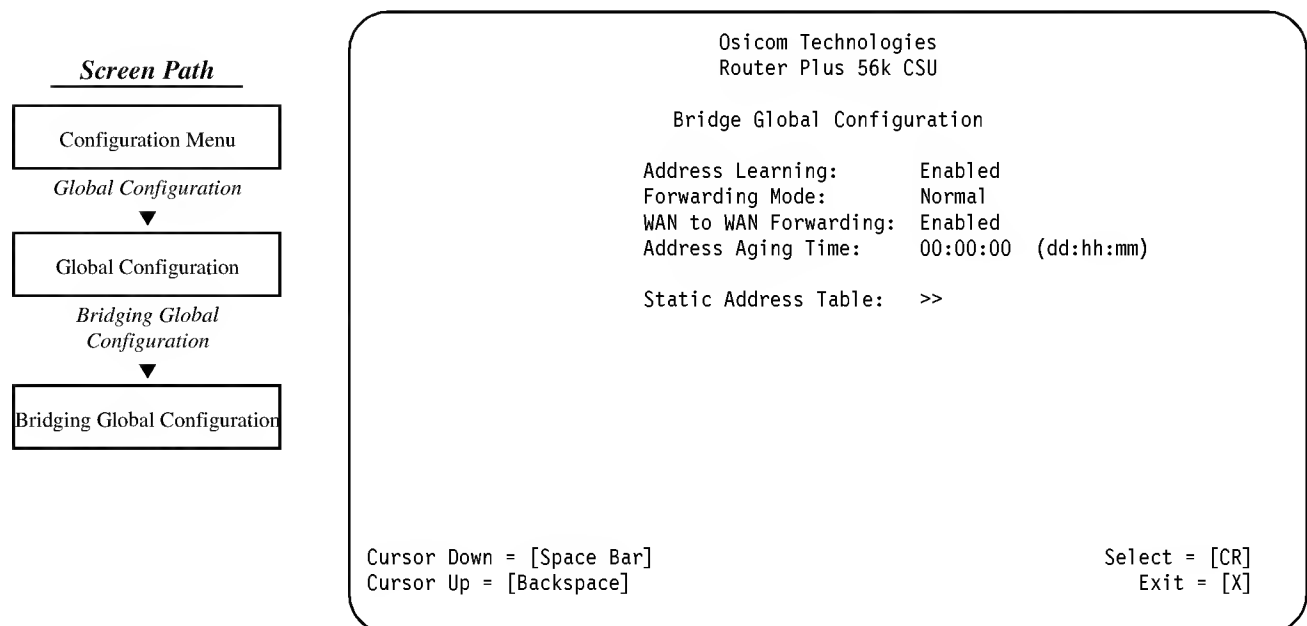


Figure 5-33. Bridging Global Configuration

5.6.3.1 Bridging Static Addresses

Access the bridging Static Address Table (Figure 5-34) to display static addresses and to access the Static Address configuration screen.

When address learning is disabled, the bridge forwards only those frames that are to MAC Addresses configured in this table.

When address learning is enabled, the bridge forwards all frames except those that are to or from addresses that are both in the Static Address Table and are set to *Filtered*.

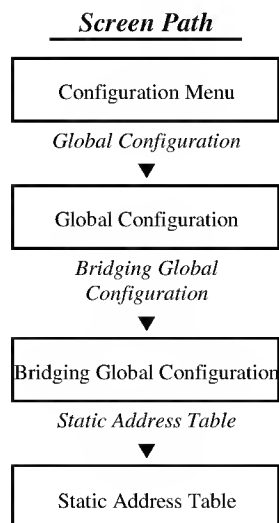
Forwarding and filtering are applied to a frame when the frame is received.

There can be up to 60 entries in the Static Address Table. When there are more than 15 entries, press **[Page Down]** or **[+]** and **[Page up]** or **[-]** to scroll between pages of addresses.

To add or edit an entry:

1. Position the cursor on the desired entry number and press **[CR]**; the Static Address configuration screen (Figure 5-35) is displayed.
2. At the Static Address configuration screen, configure each parameter as required.
3. Press **[X]** to return to the Static Address Table.

To delete an entry, move the cursor to the desired entry number and press **[D]**.



Osicom Technologies Router Plus 56k CSU			
Static Address Table - Page 1			
	MAC Address	Action	Port
1.	00:00:6d:00:30:00	Filter	--
2.	00:00:6d:00:30:01	Filter	--
3.	00:00:6d:00:30:55	Forward	1
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
Cursor Down = [Space Bar]		Delete = [D]	Select Menu = [CR]
Cursor Up = [Backspace]		Page = [+] [-]	Exit = [X]

Figure 5-34. Static Address Table

MAC Address - the Ethernet address (48-bit hexadecimal text) for the entry. Frames from or to this device are filtered or forwarded depending on the setting of the **Action** field. Setting the address to 0 deletes the entry.

Range: 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF

Default: 00:00:00:00:00:00

Action - disposition of frames either destined to or sourced from the specified MAC Address, as follows:

Filter - all frames to or from the specified MAC Address are filtered (not forwarded).

Forward - all frames destined for the specified MAC Address are forwarded to the specified port. See **Port**, following.

Default: *Forward*

Port - port number where frames are forwarded based on their destination address. Frames that contain the specified MAC address in the frame's destination field are forwarded to this port; frames that contain the specified MAC address in the source field should be received on this port. The Port value is ignored when the Action is set to Filter.

Valid range: 0 - 14

Default: 0

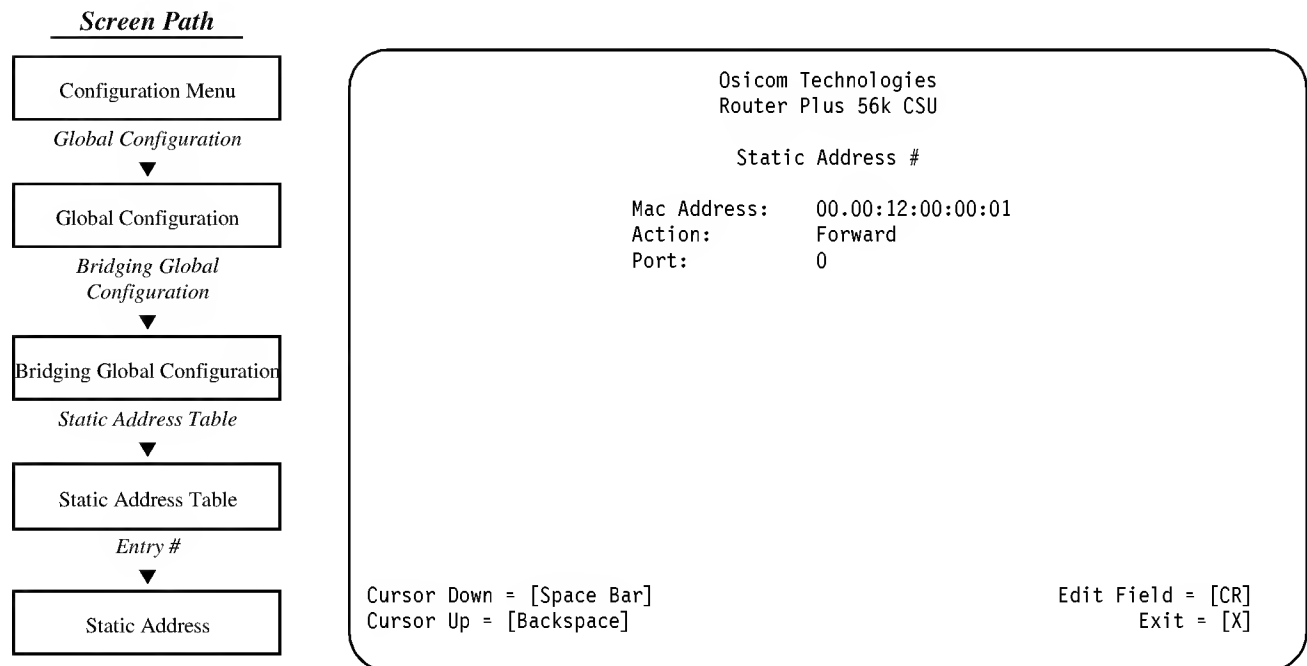


Figure 5-35. Static Address Configuration

5.6.4 PPP Global Configuration

Access the PPP Global Configuration screen to configure global PPP options as shown in Figure 5-36.

When you press **[CR]** at an option, follow the prompts at the bottom of the screen.

Restart Timer - used to time transmissions of Configure-Request and Terminate-Request packets. Expiration of the Restart timer causes a Timeout event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.

Valid input: *1 to 10 seconds*

Default: *3 s*

Maximum Number Of Termination Requests - the number of Termination Request packets that can be sent without receiving a Terminate Acknowledge, before assuming that the peer is unable to respond.

Valid input: *1 to 100*

Default: *2*

Maximum Number Of Configuration Requests - the number of Configuration Request packets that were sent without receiving a valid Configuration Acknowledged, Configuration Not Acknowledged, or Configuration Reject before assuming that the peer is unable to respond. When this threshold is reached, the counter is reinitialized and the link initialization is started again.

Valid input: *2 to 100*

Default: *10*

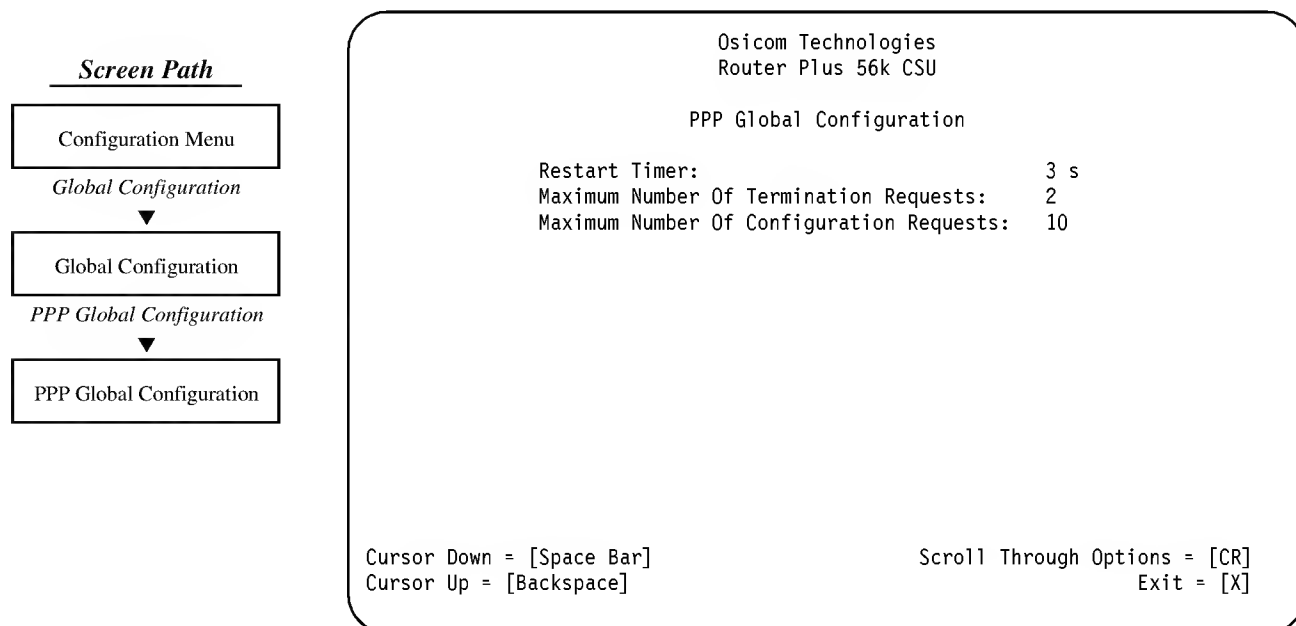


Figure 5-36. PPP Global Configuration

5.6.5 Encryption Global Configuration

Use this screen to configure global encryption options.

Key Update Time - the time at which all Pending Keys will become the active Current Keys. Its purpose is to synchronize the changing of the DES encryption keys of all interconnected routers. Only ports with encryption enabled are updated.

Valid input: 00:00:00 to 24:00:00 (HH:MM:SS)

Default: 00:00:00 (disables timer)

To use this timer, perform these steps for each router using encryption:

1. Make sure the router's clock is set correctly.

2. Configure Pending Keys for each port. See Encryption Options on page 5-37.
3. Set this option for the time of day to update the encryption keys.
4. Exit the screen and confirm the configuration.

When the system time reaches the Key Update Time, the Key Update Time is reset to 00:00:00 and all pending keys on ports with encryption enabled automatically overwrite the current keys.

Valid input: 00:00:00 to 24:00:00 (hh:mm:ss)

Default: 00:00:00 (disables this feature)

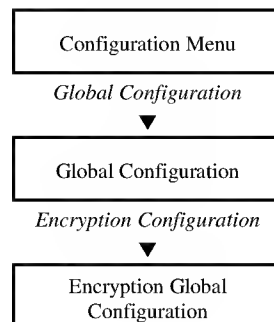
NOTE

To ensure synchronization, the system time for all communicating units should be set for the same time regardless of differences in time zones. Otherwise, the pending keys overwrite current keys at different times for different units, thus preventing communication between the units.

NOTE

When the time set for **Key Update Time** is reached, all configuration settings are saved automatically (firmware version 2.0.10 and later). This ensures that the newly updated **Current Key** configuration is retained following a re-boot or power interruption.

Screen Path



12:30:00
Osicom Technologies
Router Plus 56k CSU
12:00:00

Encryption Global Configuration

Key Update Time:
12:30:00 (hh:mm:ss)

NOTE

If a DES-KEY-LIC (encryptor key license) has been purchased and implemented, two additional selections will appear on this screen when the user enters the appropriate password upon accessing the management screens.

- Master Key Configuration
- Initial Vector Configuration

See *Ordering Information* in Appendix D.

Cursor Down = [Space Bar]

Cursor Up = [Backspace]

Edit Field = [CR]

Exit = [X]

Figure 5-37. Encryption Global Configuration

CONFIGURATION AND SOFTWARE UPDATE (TFTP) 6

This chapter illustrates and describes the router's Configuration and Software Update screens. Access these screens to transfer configuration and software files between the router and a TFTP (Trivial File Transfer Protocol) server. Configuration and software file transfers can be performed across the LAN or WAN from a local or remote server.

Software files contain the operating system; configuration files consist of the parameters and options.

After reading this chapter, the user will be able to *send* files to a TFTP server and *get* files from a TFTP server.

6.1	Screen Structure	6-1
6.2	Configuration and Software Update	6-2

6.1 Screen Structure

The organization of the **TFTP** screens is shown below. Position the cursor on the TFTP selection at the Main Menu and press **[CR]** to access the Configuration and Software Update screen (Figure 6-2).

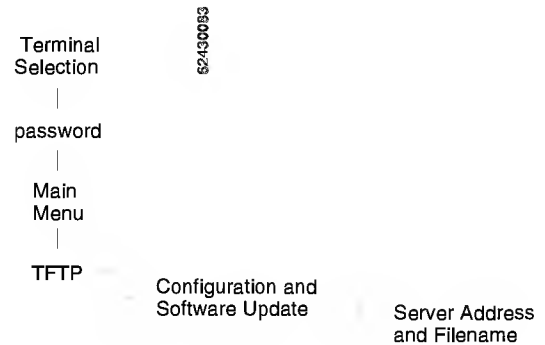


Figure 6-1. Screen Structure (TFTP)

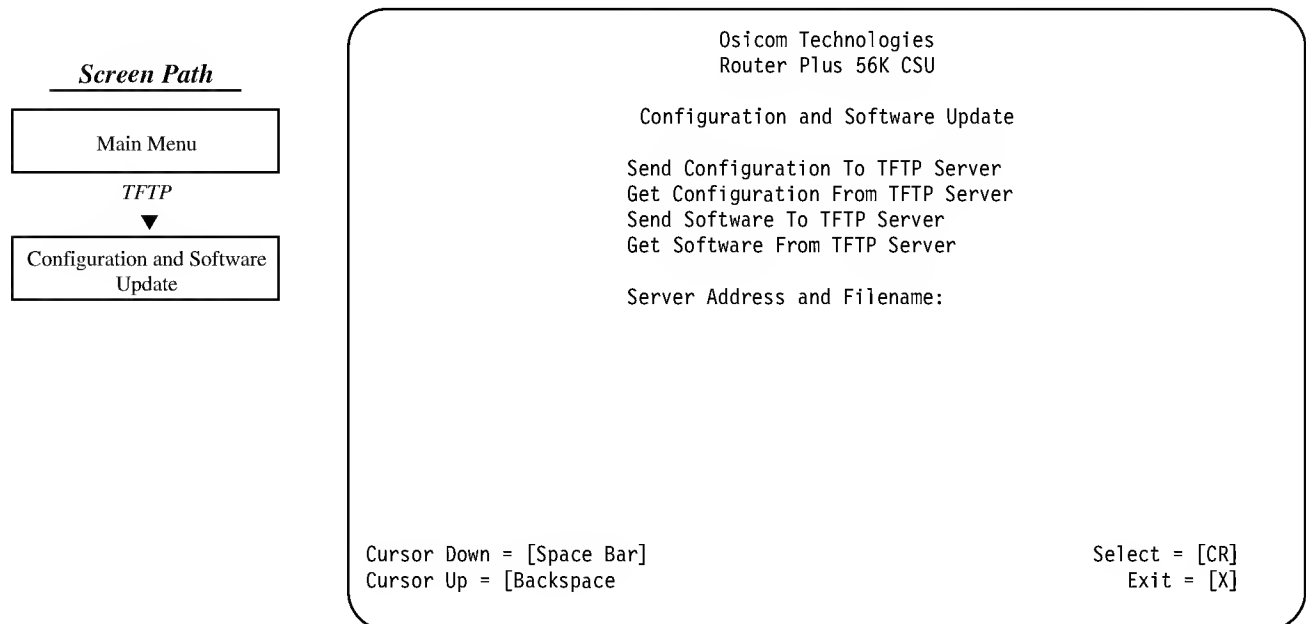


Figure 6-2. Configuration and Software Update

6.2 Configuration and Software Update

NOTES

1. Only the Routermate Plus 56K CSU version with SIMM (extended memory) can get software files while running the main software. The **Get Software From TFTP Server** command is not displayed on the router version without SIMM.

To get software from a TFTP server on a unit without SIMM installed, select the **Restart SW Download - Use Database** command on the System Restarts menu, which is accessed from the Unit screen (see Chapter 8).

2. If sending a file to the server, the file must already exist on the server, and the file must have read/write privileges for everyone.
3. An unreliable file will result if the file on the server is larger than the file being sent. The file being sent will not overwrite the entire file on the server; instead, the file being sent will overwrite only a portion of the file on the server. The result will be a file made up of parts of both files.

1. Enter the server's address and filename on the Server Address and Filename configuration screen (Figure 6-3).
2. Press **[X]** to return to the Configuration and Software Update screen.

Screen Path

Configuration and Software Update

Server Address and Filename



Server Address and Filename

If a transfer is attempted without setting the Server Address and Filename, the following messages may be displayed:

- ▶ Filename Missing
- ▶ Server Address Missing
- ▶ Filename and Server Address Missing

When this occurs, the cursor is positioned on the Server Address and Filename choice. Press **[CR]** to display the Server Address and Filename configuration screen.

Server Address - server's IP address.

Default: 0.0.0.0 (not configured).

Filename - text string; alphanumeric, 50 characters maximum.

Default: Blank (not configured).

Gateway Address (only displayed for version without SIMM) - configure this address when the server is on a remote network. Enter the address of the router that leads to the remote server. Only required when you select the **Restart SW Download - Use Database** command on the System Restarts screen (see Chapter 8).

Default: 0.0.0.0 (not configured).

```

Osicom Technologies
Router Plus 56K CSU

Server Address and Filename

Configuration File

Server Address:  0.0.0.0
Filename:        /filename.txt

Software File

Server Address:  101.100.100.100
Filename:        1234567890123456789012345678901234567890
Gateway Address: 100.100.100.100

Cursor Down = [Space Bar]      Edit Field = [CR]
Cursor Up   = [Backspace]      Exit   = [X]

```

Figure 6-3. Server Address and Filename (w/o SIMM)

Position the cursor on the desired *Send* or *Get* command and press **[CR]** to initiate the file transfer.

To abort the file transfer, press either **Ctrl-X**, **Ctrl-N**, or **Ctrl-T**.

If a transfer is stopped, the user should wait until the server times out before initiating another TFTP session.

NOTE

Selecting any command causes a status message and percentage complete prompt to be displayed. When the transfer is complete or stops, the percentage complete is cleared.

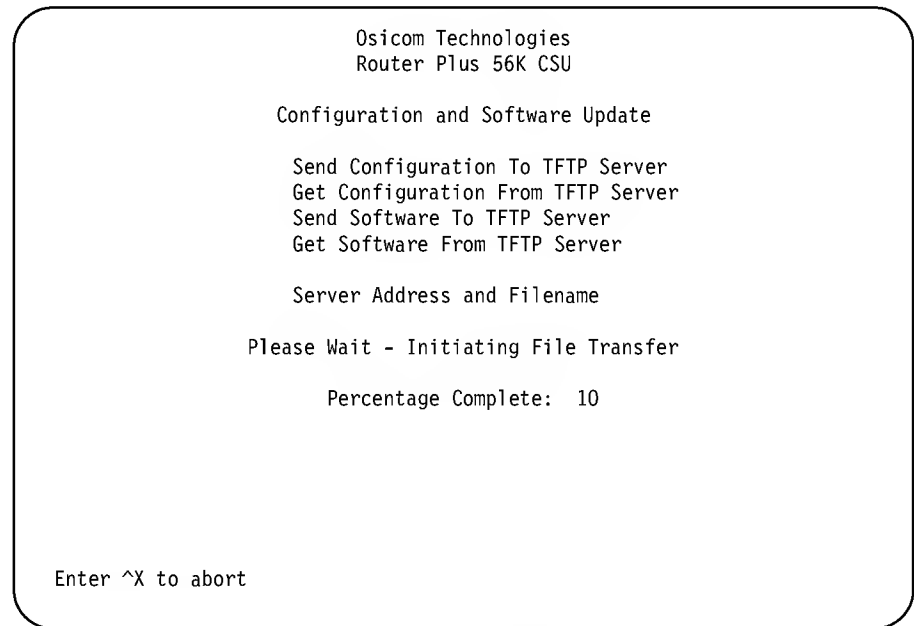


Figure 6-4. Initiating File Transfer

Figure 6-5 illustrates a **Get Configuration From TFTP Server** process.

If you select *Yes* to "Save Download to Flash," the configuration download is saved to flash and you are prompted to restart.

If you select *No* to "Save Download to Flash," the configuration download is deleted from RAM and the file transfer is discarded. The cursor returns to the **Get Configuration From TFTP Server** command.

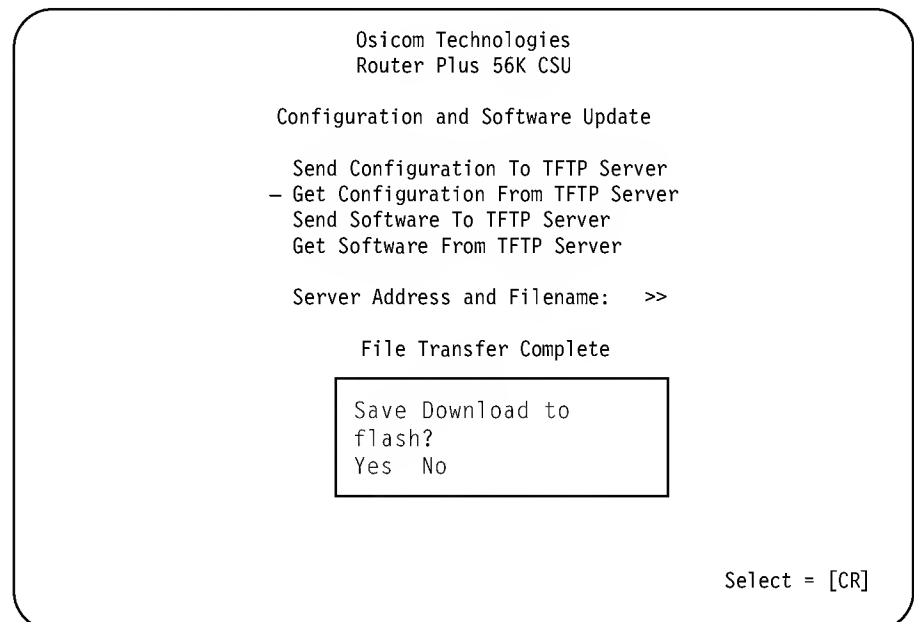


Figure 6-5. Configuration File Transfer

Figure 6-6 illustrates a **Get Software From TFTP Server** process on a Routermate Plus 56K with SIMM installed. If you select *Yes* to "Save To Flash and Restart," the software download is saved to flash and the router is restarted using the new software.

If you select *No* to "Save To Flash and Restart," the software download is deleted from RAM and the file transfer is discarded. The cursor returns to the **Get Software From TFTP Server** command.

```

Osicom Technologies
Router Plus 56K CSU

Configuration and Software Update

Send Configuration To TFTP Server
Get Configuration From TFTP Server
Send Software To TFTP Server
- Get Software From TFTP Server

Server Address and Filename:  >>

File Transfer Complete

Save To Flash and
Restart?
Yes No

```

Figure 6-6. Software File Transfer

Figure 6-7 illustrates a **Send Software To TFTP Server** process.

If the file transfer fails, the "cause of failure" is displayed.

A **Send Configuration To TFTP Server** process operates the same way.

```

Osicom Technologies
Router Plus 56K CSU

Configuration and Software Update

Send Configuration To TFTP Server
Get Configuration From TFTP Server
- Send Software To TFTP Server
Get Software From TFTP Server

Server Address and Filename

File Transfer Complete

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Select = [CR]
Exit = [X]

```

Figure 6-7. Software File Upload

This chapter illustrates and describes the router's Modem configuration menu. This screen will appear only if the optional V.32 modem is installed. Use this screen to configure the modem for dial-in management of the router's console screens. Dial-in console access takes priority over local console and Telnet access.

This text also serves as a reference tool for defining the various parameters and options appearing on the screens.

7.1	Screen Structure	7-1
7.2	Modem Parameters	7-2

7.1 Screen Structure

The organization of the **Modem** menu is shown below. Position the cursor on the Modem selection at the Main Menu and press **[CR]** to access the Modem menu.

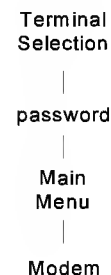


Figure 7-1. Screen Structure (Modem)

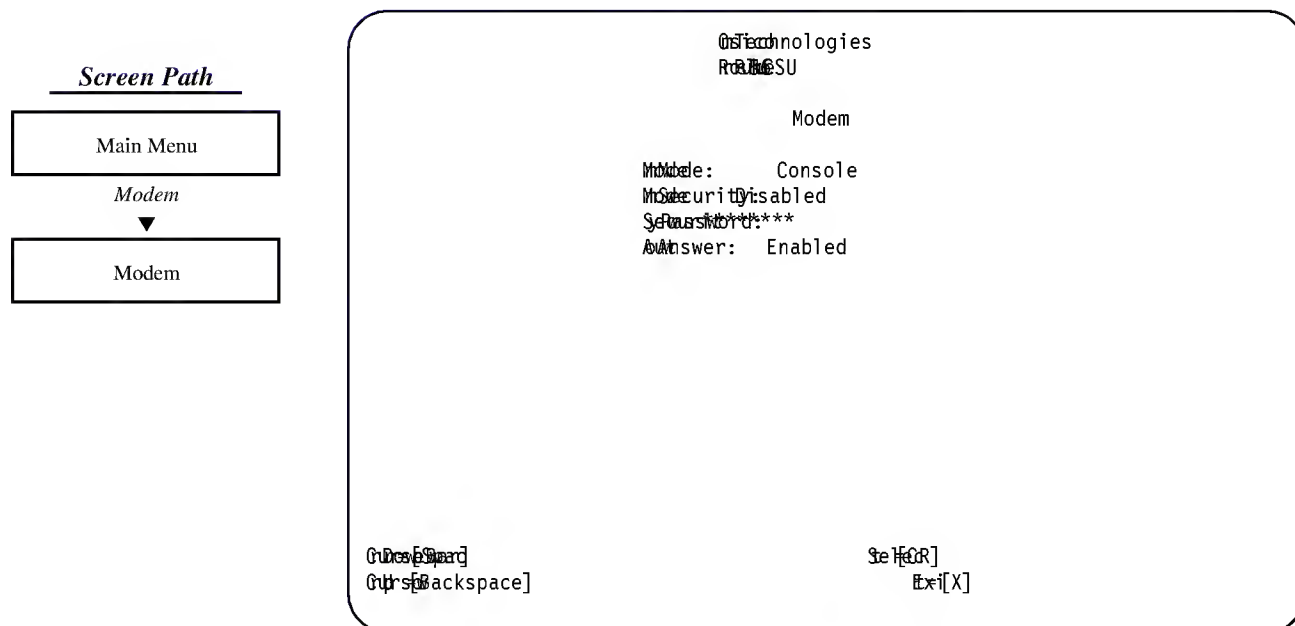


Figure 7-2. Modem Menu

7.2 Modem Parameters

Modem Mode - access the WAN 2 interface or the console screens of the router. This parameter is currently fixed at Console. Dial-in console access takes priority over local and Telnet console access.

Default: *Console*

Modem Security - enable/disable security password to access the router through the modem.

Default: *Disabled*

NOTE

If using Osicom's 4532 or 4232 modem, you can enable **Modem Security** to prevent an unauthorized connection. If using a modem other than Osicom's 4532 or 4232 modem, **Modem Security** must be disabled.

Security Password - the password exchanged between the integral modem and the calling 4532 or 4232 when **Modem Security** is enabled.

Valid input: up to eight alphanumeric characters; case sensitive.

Default: *password*

Auto Answer - enable/disable the integral modem to automatically answer a dial-up call. This parameter must be enabled to allow dial-up access to the management screens.

Default: *Enabled*

This chapter illustrates and describes the router's Unit menu. Use this screen to configure the following supervisory functions:

- Header lines on the terminal screens
- Inactivity timeout
- System time
- Passwords (console, encryption, and dial-in management)

Also access the **System Restart**, **System Information**, and **Service Information** screens.

This text also serves as a reference tool for defining the various parameters and options appearing on the screens.

8.1	Screen Structure	8-1
8.2	Unit Parameters	8-2
8.2.1	System Restart	8-3
8.2.2	System Information	8-6
8.2.3	Service Information	8-7

8.1 Screen Structure

The organization of the **Unit** menu is shown below. Position the cursor on the Unit selection at the Main Menu and press **[CR]** to access the Unit menu.

Figure 8-2 illustrates the Unit screen for a router with an integral modem for dial-in management and encryption hardware installed.

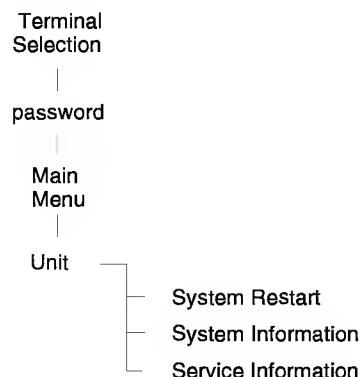
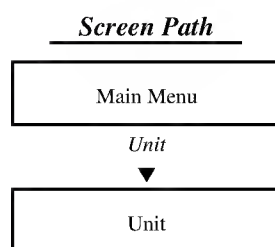


Figure 8-1. Screen Structure (Unit)



NOTE

Parameters will differ depending upon hardware options installed.

```

@Technologies 12:00:00
Router SU

Unit

Header @Technologies
Header Router SU
Inactivity timeout (mm)
Password: *****
System: 00:00:00:ss
Password: *****

System restarts >>
System information:
Service information:

Press [Space] to go to the next screen
Press [Backspace] to go to the previous screen
Press [CR] to edit
Press [X] to exit
  
```

Figure 8-2. Unit Menu

8.2 Unit Parameters

Use the Unit screen to edit the two header lines that appear on all screens and perform other supervisory functions.

Also access the System Restart screen (page 8-3), the System Information screen (page 8-6), and Service Information screen (page 8-7).

To configure a parameter by typing a value:

1. Press the **[Space Bar]** or **[Backspace]** to move the cursor to the desired parameter.
2. Press **[CR]** to highlight the field.
3. Type the value.
4. Press **[CR]** again to exit the field.

To restore the parameter to its original contents, press **[Esc]** before exiting the field.

Unit menu parameters are defined below. Note that certain parameters are displayed only for specific hardware versions of the Routermate Plus.

Header Line 1, Header Line 2 - these two fields let you modify the text that appears in the first two lines of each screen. Press **[CR]** to highlight the field, enter the new header, then press **[CR]** again when you are finished.

Valid input: Up to 40 alphanumeric characters; spaces are permitted anywhere in the field.

Default: *Osicom Technologies*
Router Plus 56k CSU

Inactivity Timeout - time, in hours and minutes, during which if there is no keyboard activity, the console is deactivated, or the Telnet connection is terminated. This parameter is for terminal and Telnet users only. Access to the management screens is then restricted to persons who can enter the password.

Valid input: 00:00 (disables timer) to 23:59. Type the time as a continuous 4-digit number in the format hh:mm. You do not have to type the colon.

Default: 00:05

Console Password - for terminal and Telnet operation only; sets a password that restricts access to the management screens. Entering the Console Password allows the user access to all the screens except the encryption screens.

Valid input: Up to 16 alphanumeric characters, case-sensitive. Spaces can be used, but a space cannot be used as the first or last character.

A Telnet user has three attempts and thirty seconds to enter the correct password; if unsuccessful, the session is disconnected.

Default: [CR]

System Time (displayed only when encryption option is installed) - the system time in hours (hh) minutes (mm) and seconds (ss). You do not have to type the colons [:]. When configured, the time is displayed in the upper, right corner of the screens.

Key Password (displayed only when encryption hardware is installed) - enter the Key Password for access to all the screens.

Valid input: Up to 16 alphanumeric characters, case-sensitive. Spaces can be used, but a space cannot be used as the first or last character.

To configure the password, press **[CR]** to highlight the field, and type the new password. If you make a typing error use **[Backspace]** to move the cursor to the left, and re-type the correct characters. Press **[Esc]** before exiting the field to return the password to its previous setting. Press **[CR]** to exit the field after typing the new password.

The new password is not displayed on the screen. A string of asterisks (*) indicates that a password is configured.

A Telnet user has three attempts and thirty seconds to enter the correct password; if unsuccessful, the Telnet session is disconnected.

Default: [CR]

8.2.1 System Restart

The System Restart screen supports four types of restarts, including two with software downloads. The screen shown in Figure 8-3 is for a unit without SIMM. The **Restart SW Download - Use Database** is not displayed on Routermate Router Plus 56K units with SIMM.

Selecting a restart command causes a confirmation box to appear. If you select **Yes**, the following message appears:

Please wait - type of restart in progress

NOTES

A Telnet session is closed once any restart is initiated. Following a defaults restart, you must re-enter the IP address from a local terminal before another Telnet connection can be made.

Cancel - exit the screen.

System Restart - this restart is equivalent to powering the router off and on. Configuration parameters are not affected.

Defaults Restart - select this option to change all configurable parameters to their default values. This includes the Console and Key passwords but does not include the Master key or Initial Vector passwords.

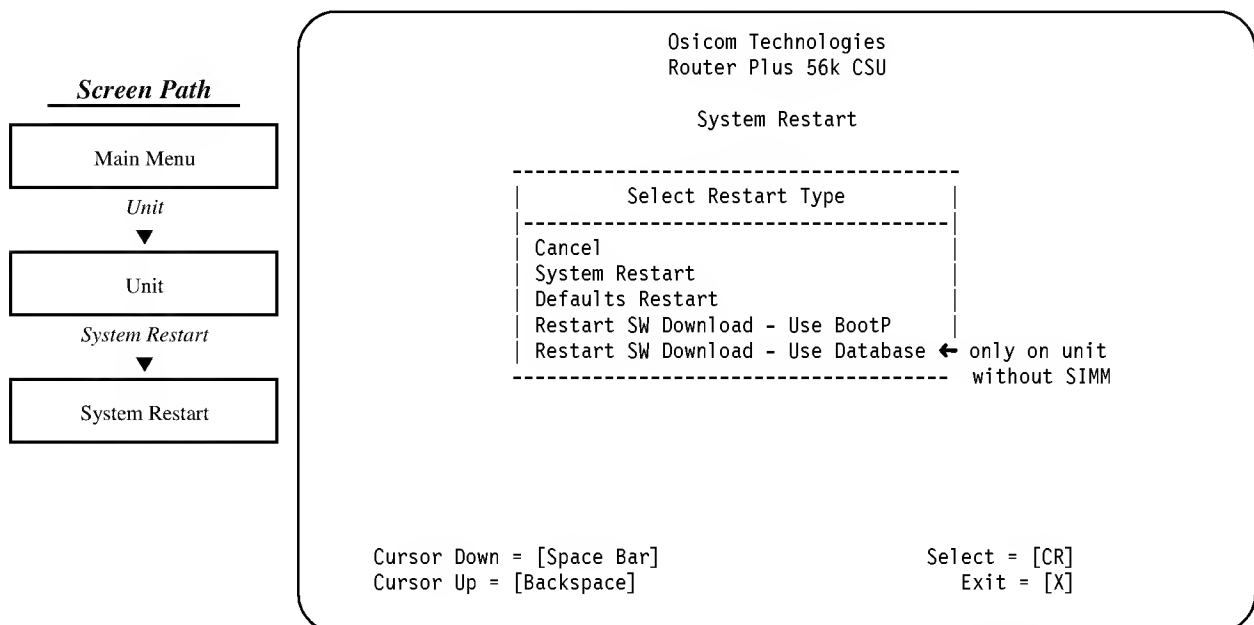


Figure 8-3. System Restart (Without SIMM)

Restart SW Download - Use BootP - when this command is selected, the router restarts, runs the boot image, and sends out a BootP request. The information in the BootP response is used to automatically perform the TFTP transfer. Once the image file is successfully transferred, the unit runs the full image and uses the configuration stored in the database, including the LAN IP address. If the transfer is unsuccessful, the unit discards the file and runs the existing full image.

The advantage of using this command over the **Get Software From TFTP Server** in the TFTP menu (see Chapter 6) is that the server address and filename do not need to be known.

NOTES

1. **Restart SW Download - Use BootP** command can only be performed across the LAN because the WAN is not operational when running from the boot sector.
2. The **Restart SW Download - Use BootP** command can only be used to retrieve a file from a remote server if the router that leads to the remote BootP server supports BootP Relay.

Restart SW Download - Use Database - (Only displayed on router version without SIMM. This additional command is provided because the version without SIMM does not have enough memory to store a downloaded software image file and run the full image at the same time.

When this command is selected, the router restarts and attempts to get the image file. Once the image file is successfully transferred, the unit runs the full image and uses the configuration stored in the database, including the LAN IP address. If the transfer is unsuccessful, the unit discards the file and runs the existing full image. See the Server Address and Filename screen in Chapter 6 to configure addresses for TFTP transfers.

NOTES

1. The **Restart SW Download - Use Database** command can only be performed across the LAN because the WAN is not operational when running from the boot sector.
2. You can download through another router on the local LAN if you configure the LAN address of the other router as the Gateway Address. See *Configuration and Software Update* in Chapter 6.

Osicom Technologies
Router Plus 56k CSU

System Restart

Select Restart Type

Cancel
System Restart
Defaults Restart
Restart SW Download - Use BootP

Confirm Restart?

No Yes

Cursor Down = [Space Bar]
Cursor Up = [Backspace]

Select = [CR]
Exit = [X]

Figure 8-4. System Restart (With SIMM)

Figures 8-5 and 8-6 illustrate a restart and software download in progress.

Software download can only be performed across the LAN because the WAN is not operational when running from the boot sector.

```
Osicom Technologies
Router Plus 56k CSU

System Restart

-----
Select Restart Type
-----
Cancel
System Restart
Defaults Restart
Restart SW Download - Use BootP
-----

Please wait - Restart SW Download in progress
```

Figure 8-5. System Restart (SW Download in Progress)

The message shown in Figure 8-6 is displayed if any restart command is selected when there are unsaved configuration changes. Selecting **No** clears the message and returns the cursor to last position.

```
Osicom Technologies
Router Plus 56k CSU

System Restart

-----
Select Restart Type
-----
Cancel
System Restart
Defaults Restart
Restart SW Download - Use BootP
-----

-----
Unsaved configuration changes - continue restart?
No      Yes
-----
```

Figure 8-6. System Restart (Prompt for Unsaved Configuration Changes)

8.2.2 System Information

Select **System Information** at the Unit screen to view the System Information screen (Figure 8-7).

This screen displays software and hardware options integral to the router.

Software Version - the revision level of the router's firmware.

Software Checksum - 32-bit CRC checksum of operational software.

Boot Sector Version - the revision level of the boot sector firmware.

WAN 2 Daughter Card Type - hardware option for WAN 2 interface.

Valid options: *None, V.32, ISDN U*

Encryption Daughter Card Type - hardware option for encryption.

Valid options: *None, Standard, High Performance, Proprietary Standard, Proprietary High Performance*

Compression Daughter Card Type - hardware option for compression.

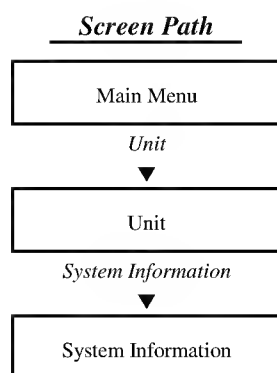
Valid options: *None, Standard, High Performance*

RAM Size - number of bytes of memory.

Valid options: *1 M (without SIMM)
4 M (with SIMM)*

Flash Size - number of bytes of memory used to store configuration and software image files.

Valid options: *1 M or 2 M*



Osicom Technologies
Router Plus 56k CSU

System Information

Software Version:	2.x.xx
Boot Sector Version:	2.x.xx
WAN 2 Daughter Card Type:	V.32
Encryption Daughter Card Type:	High Performance
Compression Daughter Card Type:	None
RAM Size:	4 M
Flash Size:	1 M

Exit = [X]

Figure 8-7. System Information

8.2.3 Service Information

Select **Service Information** at the Unit screen to display the Service Information screen (Figure 8-8).

This screen provides address, telephone, fax, e-mail, and web site numbers for contacting service personnel.

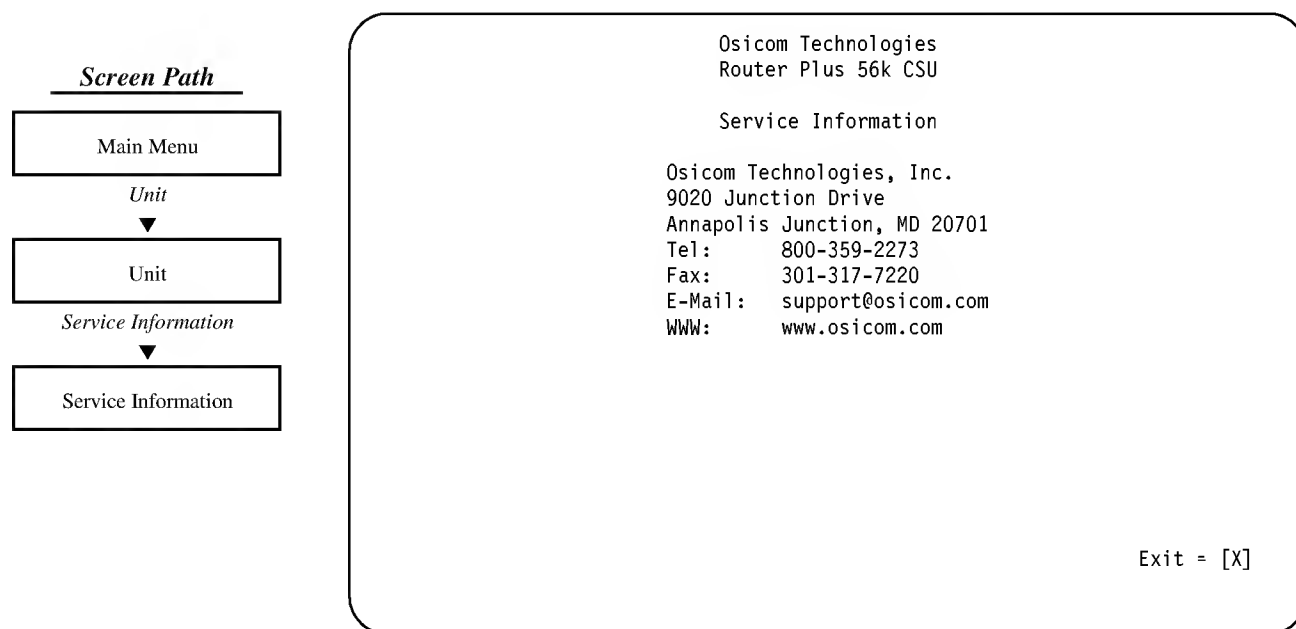


Figure 8-8. Service Information

This chapter describes the router's Management menu. Use this screen to enable Telnet access, configure SNMP (Simple Network Management Protocol) options, and access the **SNMP Trap Client Table**.

This text also serves as a reference for defining the parameters and options appearing on the screens.

NOTE

SNMP management capabilities:

- Router - standard MIB II
- CSU - enterprise MIB
- Encryption - enterprise MIB

9.1	Screen Structure	9-1
9.2	Management Parameters	9-2
9.2.1	SNMP Trap Client Table	9-2
9.2.2	Traps	9-3

9.1 Screen Structure

The organization of the **Management** menu is shown below. Position the cursor on the Management selection at the Main Menu and press **[CR]** to access the Management menu.

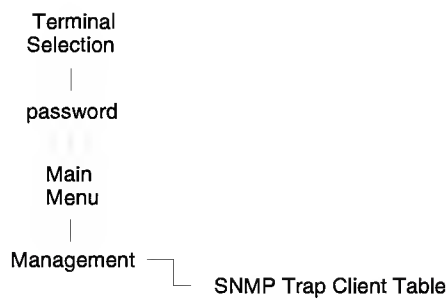


Figure 9-1. Screen Structure (Management)

Screen Path

Main Menu

Management

▼

Management

Router Technologies
Router CSU

Management

Telnet Server: Enabled
SNMP Community public
SNMP Community private
Authentication Disabled
Authentication Enabled
SNMP Enable:

Cursor [Tab]
Cursor [Backspace]

Set [CR]
Exit [X]

Figure 9-2. Management

9.2 Management Parameters

Telnet Server - enable/disable Telnet access to the management screens.

Default: *Enabled*

SNMP R/O Community - the community string used for read-only access to the router's MIB objects.

Valid input: Up to 40 alphanumeric characters

Default: *public*

SNMP R/W Community - the community string used for read-write access to the router's MIB objects. If this is set to the same value as the read-only string, write access is prevented.

Valid input: Up to 40 alphanumeric characters.

Default: *private*

Authentication Traps - enable/disable authentication traps sent by the router when an SNMP request is received with an invalid community string. A trap is an unsolicited alarm or event.

Enabled - allows alarm messages.

Disabled - prevents alarm messages.

Default: *Disabled*

Autolearn Clients - enable/disable the router's ability to automatically learn the IP addresses of SNMP management stations (clients) to whom SNMP traps are to be sent.

Enabled - the SNMP Trap Client Table lists the management stations that will receive traps from the router. The router automatically learns the IP addresses of SNMP management stations that access it. Learned addresses are added to the table, which can contain up to 16 addresses. If the table contains any static addresses, then the number of addresses that can be learned is 16 minus the number of configured static addresses.

Disabled - the SNMP Trap Client Table lists the management stations that can access the router's SNMP agent, and the management stations that will receive traps from the router. SNMP access is limited to only the hosts that are listed in the table. See the **SNMP Trap Client Table** in the following section.

Default: *Enabled*

9.2.1 SNMP Trap Client Table

A trap client is an SNMP management station to which SNMP traps are routed. A trap client is identified by configuring an IP address for each of up to 16 SNMP management stations.

Move cursor between columns by using left/right arrows or Tab/Shift-Tab.

IP addresses for trap clients can be configured manually, or automatically learned.

For automatic address learning, see **Autolearn Clients** in previous section. Any addresses that are not entered manually can be learned automatically.

Trap client addresses can be configured manually using SNMP management or from a terminal at the SNMP Trap Client Table screen.

If it is desirable to limit the management stations to which traps are sent, the IP addresses for those management stations can be configured manually and the autolearn feature disabled. Only those management stations whose IP addresses have been configured manually will receive traps from the router.

Client Address - the IP address for the SNMP management station to which SNMP traps are to be sent. Default value is 0.0.0.0 (no entry configured).

Type - the Type field is read only. It identifies a trap client as one of the following:

Dynamic - the IP address for this trap client was learned automatically from an incoming SNMP message.

Static - the IP address for this trap client was configured manually.

----- no address is assigned.

9.2.2 Traps

A trap, which is the SNMP term for an alarm or event, is unsolicited information from an SNMP agent to an SNMP management station. Traps are the only type of unsolicited data that is permitted with SNMP. A trap occurs only when a threshold within the agent is violated or when a major event occurs.

The following MIB-II traps also are reported:

- Link Up
- Link Down
- Warm start
- Cold start
- Authentication

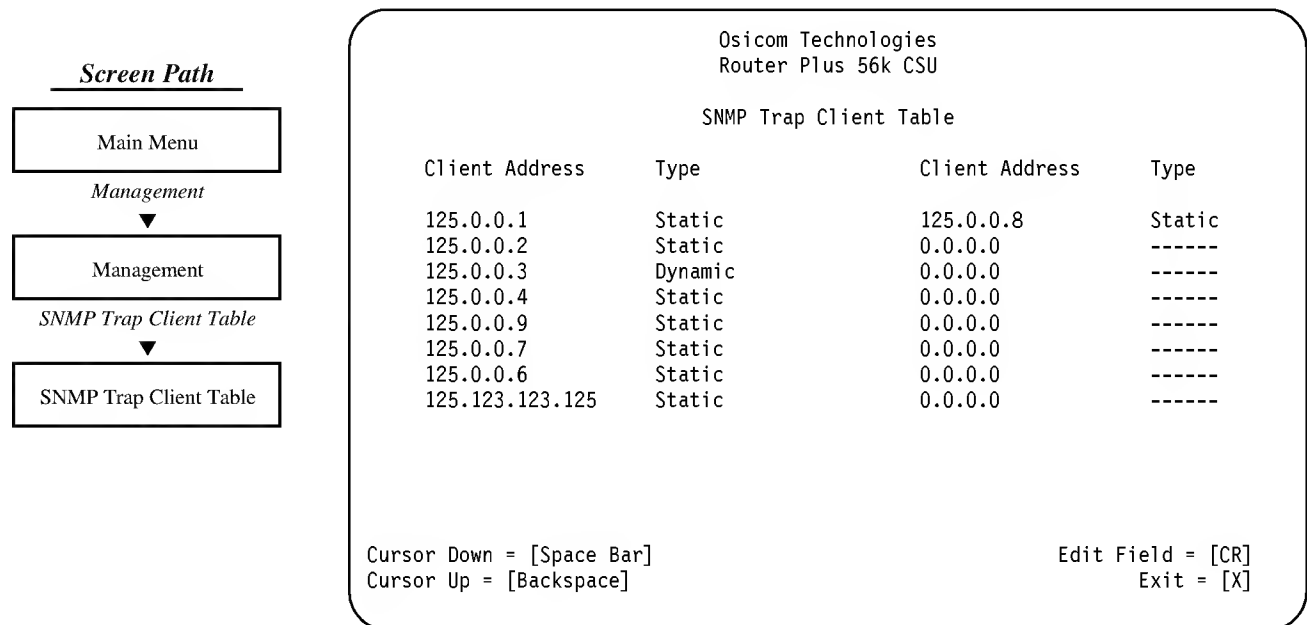


Figure 9-3. SNMP Trap Client Table

10.1 Customer Support

Osicom Technologies offers a comprehensive range of customer support services, including technical assistance and maintenance agreements.

For technical assistance or detailed information about Osicom's support plans or pricing, call 1-800-DLX-CARE (1-800-359-2273) to reach a Customer Service Marketing Representative.

The Service Information screen, accessed from the Unit menu, provides fax and web site numbers.

10.2 Equipment Return and Repair

Corrective maintenance is limited to the testing and troubleshooting procedures provided in this manual. If, after contacting Customer Support, you are unable to correct any malfunction, please return the unit to Osicom Technologies for repair.

Prior to shipping the unit to Osicom for repair, call Product Repair at 301-317-7400 and request a Return Goods Authorization (RGA) number.

You may furnish information on defective units to Osicom by telephone. Please provide the following information:

- Unit part number and serial number
- Brief description of failure symptoms and cause
- Return shipping address (including sender's name)
- Preference of return shipping mode
- Invoice address
- Purchase Order number or letter of authorization for out of warranty units
- Person to contact for further information. Please include telephone number.

For the best equipment protection, use the original cartons and packaging material. Send the unit to:

Osicom Technologies, Inc.
9020 Junction Drive
Annapolis Junction, Maryland 20701

ATTN: RGA # _____

10BaseT - A form of Ethernet and IEEE802.3 network cabling that uses 10 Megabits per second, baseband, twisted pair cabling.

Address Mask - See Subnet Mask.

ARP (Address Resolution Protocol) - Internet protocol uses the IP address to determine the corresponding physical address. Allows a host to find the physical address of a target host on the same physical network, given only the target's Internet address. The sender's Internet-to-physical address binding is included in every ARP broadcast; receivers update the Internet-to-physical address binding information in their cache before processing an ARP packet.

Baseband - A transmission technique used in LANs. One device at a time can communicate, and a device sends its digital signal without modification on the cable.

BootP (Bootstrap Protocol) - A TCP/IP protocol by which a device can obtain such identifying information as its own IP address or download software from a remote server.

Bridge - A special purpose, dedicated computer that connects at the MAC layer two or more segments of the same network and routes packets from one to the other.

Client - An SNMP workstation to which SNMP traps (event messages) are sent.

CSU/DSU - A combination Channel Service Unit/Data Service Unit. A CSU conditions serial synchronous data for transmission over digital networks. The CSU provides such services as transmit and receive filtering, signal shaping and balance, equalization, and loopback testing. A DSU adds bipolar conversion features to improve signal shaping and strength to make transmission virtually error free.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) - A characteristic of network hardware that operates by allowing multiple stations to contend for access to transmit by listening to see if the line is idle and also allows the hardware to detect when two stations simultaneously attempt transmission.

Datagram (see IP Datagram)

DDD (Direct Distance Dialing) - The public telephone system.

DDS (Digital Data System) - AT&T DDS service and similar digital services operating at 56 kbps.

DLCI (Data Link Connection Identifier) - A frame relay numeric identifier for the local end of a logical circuit.

Dotted Decimal Notation - The representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them.

Encryption - The conversion of information into unintelligible form (cipher) for security reasons.

Ethernet - A LAN transmission network using a bus structure, first produced by Xerox, later adopted by DEC and Intel, and later adapted to create the IEEE 802.3 and ISO 8802-3 standards.

Flash - A type of non-volatile read-write memory.

Fragment - One of the pieces that results when an IP gateway divides an IP datagram into smaller pieces for transmission across a network that cannot handle the original datagram size. IP software at the receiving end reassembles fragments into complete datagrams.

Frame Relay - A standardized interface specification that provides data transfer between routers over a WAN. Frame Relay is primarily intended for use on high-quality transmission lines, where data is received relatively free of errors. Frame Relay provides data rates of up to 2.048 Mbps. Frame Relay also allows multiple simultaneous data sessions (logical channels) across a single physical interface.

FTP (File Transfer Protocol) - An upper-layer TCP protocol that provides for the transfer of files between two dissimilar machines.

Gateway - A special purpose, dedicated computer that attaches to two or more networks and routes packets from one to the other. A gateway provides protocol conversion of routed information.

Hop Count - A measure of distance between two points in the Internet. A hop count of n means that n gateways separate the source and destination.

ICMP (Internet Control Message Protocol) - An integral part of the Internet Protocol that handles error and control messages. Specifically, gateways and hosts use ICMP to send reports of problems about datagrams back to the original source. ICMP also includes an *echo request/reply* which tests whether a destination is reachable and responding.

Internet Address - The 32-bit (dotted decimal notation) address assigned to hosts on the Internet. Actually assigned to the interconnection of a host to a physical network, the IP address consists of a network portion and a host portion.

IP (Internet Protocol) - A standardized method by which separate networks communicate; the inter-connected network is referred to as the *internet*.

IP Datagram - The basic unit of information passed across the Internet. It contains a source and destination address along with data.

IPX (Internetwork Packet eXchange) - A Novell protocol for Novell LAN communications.

ISDN (Integrated Services Digital Network) - An international digital communications standard that supports voice, data, and image applications using standard interfaces over a single telephone line.

LAN (Local Area Network) - A system for inter-connecting computer equipment within a small geographic area.

Leased lines - Permanent physical connections between two local area networks, which can be established through a DDS network.

MAC (Media Access Control) Layer - The lower of two sub-layers in layer 2 of the OSI seven-layer model.

MTU (Maximum Transfer Unit) - The largest data packet size that can be transferred across a physical network.

Multicast - A technique that allows copies of a data packet to be passed to a selected subset of destinations.

NetBIOS (Network Basic Input Output System) - The standard interface to networks on personal computers.

Numbered link - An IPX RIP network number is assigned to the WAN link.

Packet - The unit of data sent across the network. IP datagrams are often referred to as packets.

PDU (Protocol Data Unit) - Datagrams relating to Logical Link Control (LLC) transmissions.

PING (Packet InterNet Groper) - A technique used in the Internet to test reachability of destinations by sending an ICMP echo request and waiting for a reply.

Port - A logical channel mapped to a device interface; the interface might serve more than one port.

PPP (Point-to-Point Protocol) - A standardized data link level encapsulation protocol used on leased lines and dial-up WAN links.

Proxy ARP - The technique in which a device, usually a gateway, answers ARP requests intended for another by supplying its own physical address. By pretending to be another device, the gateway accepts responsibility for routing packets to it. The purpose of Proxy ARP is to allow a site to use a single IP address with two physical networks.

PVC (Permanent Virtual Circuit) - In frame relay, a logical channel between devices that crosses a frame relay network and is identified at each end by a Data Link Connection Identifier (DLCI).

RIP (Routing Information Protocol) - In IP, a protocol used to exchange routing information between hosts on the Internet. In IPX, a protocol used to exchange routing information in the Novell IPX network environment.

Router - A special purpose, dedicated computer that attaches to two or more networks at the network layer and routes packets from one to the other. A router transmits protocol-specific information.

SAP (Service Advertising Protocol) - Novell's implementation of name service, by which services such as file servers and printer servers announce themselves periodically within an IPX network.

Source Quench - When datagrams arrive too quickly for a gateway or host to process, the datagrams are discarded. Source Quench is a congestion control technique by which a device experiencing congestion sends a message back to the source of the packets causing the congestion requesting that the source either stop or slow down its rate of sending datagrams.

SNMP (Simple Network Management Protocol) - A widely-accepted protocol in the TCP/IP environment that permits the management of devices across the network. In its most basic form, SNMP allows the interchange of information between two locations. It uses UDP as its transport layer and IP address as its network layer. The SNMP management station provides the user with a way to process requests and responses into and out of SNMP protocol.

Static Address - In bridging, a permanently configured address to which frames are forwarded or, optionally, not forwarded.

Static Route - In IP, a permanently configured route between devices; a route might be permanently configured to create a route to a device that does not implement the Routing Information Protocol (RIP), or to reduce the amount of traffic required to exchange routing information.

Subnet Address - An application of the IP addressing scheme that allows a site to use a single IP address for multiple physical networks.

Subnet Mask - A bit mask used in subnetting to identify which bits in an IP address represent the network number and the host number.

TCP (Transmission Control Protocol) - The Internet standard transport level protocol that provides the reliable, full duplex, stream service on which applications depend. TCP allows a process on one host to send a stream of data to a process on another. It is connection-oriented in the sense that before transmitting data, participants must establish a connection. The Internet protocol suite is often referred to as TCP/IP because TCP is one of the two most fundamental protocols.

Telnet - The Internet standard protocol for remote terminal access. Telnet allows a user at one site to interact with a remote device as if the user's terminal is connected directly to the remote device. Telnet application programs connect to the remote device, then prompt for a login ID and password.

TFTP (Trivial File Transfer Protocol) - A simple protocol that provides for the transfer of files between machines. TFTP lacks the sophistication and error-checking of FTP, and is used for simpler tasks in circumstances where error checking is performed by other applications.

Trace route - This function records (traces) the path to a specified host or gateway.

Trap - An SNMP event message.

TTL (Time To Live) - A technique used to avoid endlessly looping packets. In the Internet, each datagram is assigned a time to live value when it is created. Gateways decrement the time to live field when they process the datagram and discard the datagram if the time to live counter reaches zero.

UDP (User Datagram Protocol) - The Internet standard protocol that allows an application program on one unit to send a datagram to an application program on another unit.

Unnumbered link - No IP network or subnetwork numbers are assigned to the WAN interface. Besides conserving IP address space, unnumbered links also decreases the size of the routing table since no direct routes are created for the WAN ports. This reduces the amount of memory required to hold the routing table and also decreases the amount of bandwidth used to send routing updates.

WAN (Wide Area Network) - A network that provides connection services over a large geographic area.

This appendix provides a reference for basic principles of routing and bridging with the Routermate Plus.

B.1	Local Area Networks	B-2
B.1.1	Ethernet	B-2
B.2	Wide Area Networks	B-3
B.2.1	Point to Point Protocol	B-3
B.2.2	Frame Relay	B-4
B.3	IP Routing	B-6
B.3.1	IP Address	B-6
B.3.2	Subnetworking	B-7
B.3.2.1	Subnet Mask	B-7
B.3.2.2	Class C Subnetworking Using RIP 1 ..	B-8
B.3.2.3	Class C Subnetworking Using Unnumbered WAN Links	B-14
B.3.3	Address Resolution	B-16
B.3.4	RIP	B-18
B.3.5	Types of IP Routes	B-20
B.3.6	IP Filtering	B-22
B.4	IPX Routing	B-23
B.4.1	Frame Types	B-23
B.4.2	Novell Addressing	B-24
B.4.3	Watchdog Spoofing	B-24
B.4.4	RIP	B-26
B.4.5	RIP Filtering	B-28
B.4.6	SAP	B-28
B.4.7	SAP Filtering	B-29

B.1 Local Area Networks

A Local Area Network (LAN) is a group of inter-connected computing devices that are confined to a relatively small physical area. LANs provide for centralized management, resource sharing, and uniformity and compatibility of devices. A LAN is a high-speed network due to the relatively short physical area it occupies, and it is privately owned.

Figure B-1 shows a simple LAN on which several personal computers share a single printer.

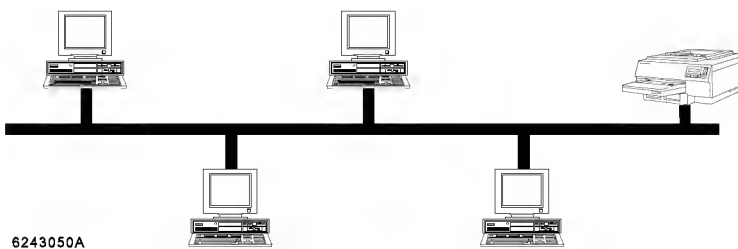


Figure B-1. Local Area Network

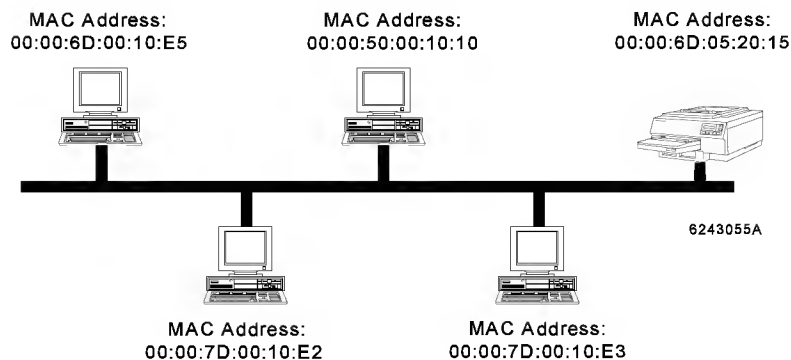


Figure B-2. MAC Addresses on a LAN

B.1.1 Ethernet

Ethernet is a LAN hardware standard that provides for linking up to 1024 nodes (stations) in a bus network. Ethernet uses a baseband (single-channel) communication technique that provides for a 10 Mbps raw data transmission rate. Ethernet uses Carrier-Sense Multiple-Access/Collision-Detection (CSMA/CD) techniques for intra-LAN communication.

Each device manufactured for use on an Ethernet LAN has designed into it during manufacture an Ethernet address, which is also known as the Media Access Control (MAC) address (Figure B-2). The manufacturer assigns the MAC address under the direction of the Institute of Electronics and Electrical Engineering, Inc. (IEEE). Devices on the Ethernet LAN use the MAC addresses to identify and communicate with each other.

B.2 Wide Area Networks

A wide-area network (WAN) provides communication links to remote sites over a public telephone service. There are numerous types of WANs.

Various connect protocols provide standards for the ways in which equipment connects to a WAN. Two connect protocols described below are:

- Point-to-Point (PPP)
- Frame Relay

B.2.1 Point to Point Protocol

The Point-to-Point Protocol (PPP) establishes a synchronous-link connection and encapsulates network-layer protocols for transmission over WAN links.

PPP provides transport services for data packet delivery with low overhead and high throughput. Frame checking at the link level offers error detection; however, error recovery is taken care of by higher layer network protocols.

With PPP, the Link Control Protocol (LCP) establishes, configures, maintains, and terminates the data-link connection.

Various Network Control Protocols (NCPs) manage the specific needs of the associated network-layer protocol.

Reference: RFC 1548, Point-to-Point Protocol (PPP) for the transmission of multi-protocol datagrams over point-to-point links.

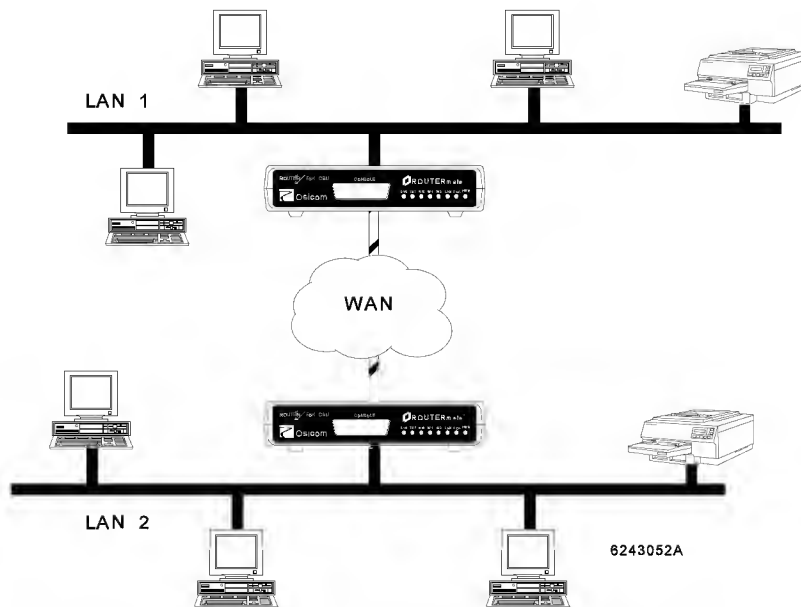


Figure B-3. Wide Area Network

B.2.2 Frame Relay

Frame relay is an interface specification. It provides a mechanism for signaling and data transfer. Frame relay service involves using frame relay access equipment which sends information across the network; this might be, for example, a router, a bridge, a host computer, etc. In public networks, frame relay switching equipment is responsible for the transportation of information across a WAN. Private frame relay switches are required for private frame relay networks.

Frame relay is designed for use on high quality transmission lines. Data is encapsulated according to the Multiprotocol Encapsulation Implementation Agreements of the Frame Relay Forum. Frame Relay accommodates burst-intensive applications, such as wide area LAN inter-connections.

Frame relay provides bandwidth-on-demand and allows multiple simultaneous data sessions (logical channels) across one physical line interface.

Frame relay can be very cost effective when used to interconnect several sites. Frame relay allows several logical links to different sites across one physical connection.

The frame relay network consists of pre-established logical links between the network's endpoints; these logical links are known as Permanent Virtual Circuits (PVCs). Since the links are pre-established, they can be used immediately whenever they are required.

Each PVC on a link is identified logically by a number called the Data Link Connection Identifier (DLCI). DLCIs are obtained from the service provider. DLCIs are used to route frames through the frame relay network. A frame forwarded to the WAN interface is transmitted on the DLCI specified by the port configuration.

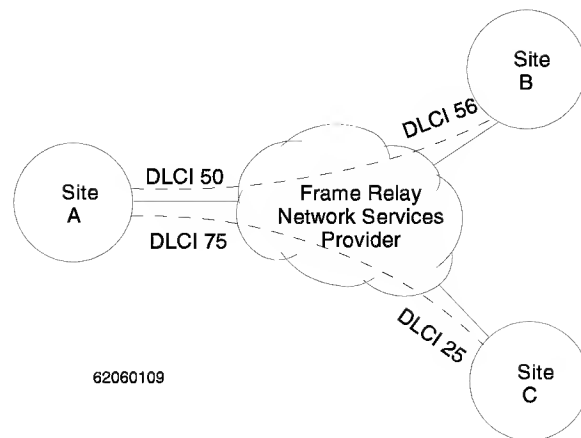
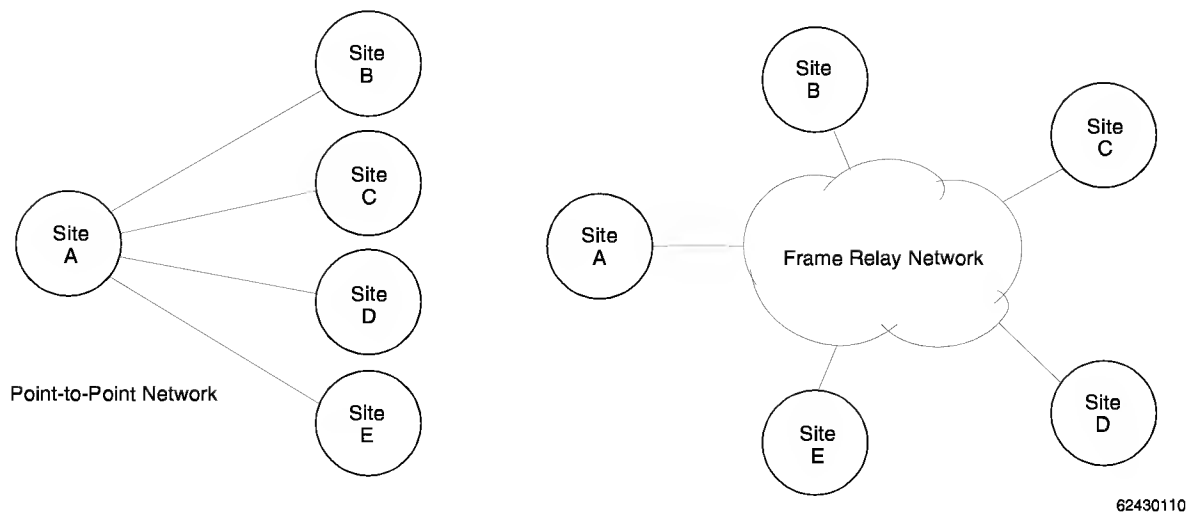
The DLCI has local significance only. For configuration purposes, the local user can think of it as identifying a particular destination but, to the network, it identifies a logical connection between the user and the local network access node. It is not a unique address for any specific destination and it can change as the frame travels through the network (see Figure B-4).

Since the frame relay network is responsible for all switching and routing, a single interface and access line can be used to address traffic to multiple destinations throughout the network.

Figure B-5 compares a PPP application to a similar frame relay application. The PPP application requires four Point-to-Point lines.

The frame relay application requires five (typically less expensive) local-access lines with a single line to each location.

The frame relay application can be more cost-effective since all connections are made through logical links rather than through leased lines.

**Figure B-4. Frame Relay Network****Figure B-5. Point to Point versus Frame Relay Network**

B.3 IP Routing

The Internet Protocol (IP) provides a standardized method by which separate networks can exchange information. The Internet Protocol refers to the interconnected networks as the *internet*, and to each communicating device on the internet as a *host*.

Each device communicating on the internet has an IP address, which is also referred to as an *internet address*. More precisely, each host *connection* to a different IP network is assigned an IP address.

B.3.1 IP Address

The IP address is a 32-bit binary number that consists of four octets. An example IP address is:

11000000 00000101 00000011 00010010

Dotted Decimal Notation - For convenience, the value for each octet in the IP address can be written in decimal integers, with the value for each octet separated by a decimal point. Such notation is referred to as *dotted decimal notation*. The expression for the above example IP address in dotted decimal notation is:

192.5.3.18

Network Number and Host Number - IP addresses are divided into two parts: a network number, and a host number.

Internet Address	
Network Number	Host Number

The network number must be unique within internet, and is assigned by the internet service provider under the direction of the InterNIC (Network Information Center) of the Internet Engineering Task Force (IETF). The network number is the same for each device on the network.

The host number must be unique within the local area network. The network owner assigns a unique host number to each device on the network.

Network Size - The network number can be contained in the first, second, and/or third octet of the IP address, depending on the size of the network. Networks are divided into three size classes according to the number of hosts that can be connected to the network:

Network Class	Number of Hosts
Class A	65,636 – 16,777,215
Class B	256 – 65,635
Class C	up to 255

The first three octets in the IP address are used for the network number, as follows:

Class A NNNNNNNN HHHHHHHH HHHHHHHH HHHHHHHH
Class B NNNNNNNN NNNNNNNN HHHHHHHH HHHHHHHH
Class C NNNNNNNN NNNNNNNN NNNNNNNN HHHHHHHH
N=Network H=Host

Class A networks are usually very large networks that contain numerous hosts (or subnetworks). The first octet of the IP address is the network number. This leaves 3 octets for up to 16,777,215 host numbers.

Class B networks are standard, large networks. Class B networks use the first two octets for the network number. This leaves two octets for up to 65,635 host numbers.

Class C networks use three octets for the network number. This leaves one octet for up to 255 host numbers.

Network Class Identification - For all networks, the first two bits in the first octet designate the network class:

Network Class	First Two Bits
Class A	00 or 01
Class B	10
Class C	11

This makes it easy for hosts to recognize the network class. By knowing the network class the host also knows which bits belong to the network number, and which belong to the host number.

Range of Network Numbers - The ranges of numbers that fulfill the above constraints and can, therefore, be assigned in the first octet for each class of network are:

Network Class	Range (Binary)	Range (Decimal)
Class A	00000000 – 01111111	0 – 127
Class B	10000000 – 10111111	128 – 191
Class C	11000000 – 11111111	192 – 255

Additional Addressing Constraints - The following additional constraints also apply to IP addressing:

- For all hosts on the same network, the part of the IP address that makes up the network number is the same.
- A host number of all binary zeroes indicates a broadcast message for all hosts on the network; therefore, a host number of all zeroes is not assigned to a host.
- A host number of all binary ones indicates a multi-cast message; therefore, a host number of all ones is not assigned to a host.

B.3.2 Subnetworking

There are not enough IP addresses to assign an IP address to all of the private LANs and individual hosts on those LANs that would like to communicate on the internet. Subnetworking techniques have resulted from the limited number of available IP addresses. When more than one network is needed, but a limited number of IP addresses are available, the necessary number of networks can be created by organizing a network into subnetworks.

The following sections present a subnetworking method for Class C subnetworking. Although Class A and Class B networks often use subnetworking, the subnetworking methods for these networks are outside the scope of this manual. For a more detailed explanation of subnetworking, the user is referred to any of the widely available texts on TCP/IP.

For a self-contained private network that does not communicate with other IP networks, subnetworking is not necessary. Self-contained private networks can use any valid network addresses and host addresses.

IP networks that communicate with other IP networks can use subnetworking to organize the local network into multiple subnetworks.

B.3.2.1 Subnet Mask

Like the IP address, a subnet mask is a 4-octet, 32-bit binary number that can be expressed in dotted decimal notation. Devices on the network compare the subnet mask to the IP address to derive the network number and the subnetwork number from the IP address.

Only certain numbers can be used as a subnet mask. The subnet mask that is selected pre-determines:

- the number of subnetworks that can be used
- the subnetwork numbers that can be used
- the number of hosts allowed on each subnetwork
- the host numbers that can be used

The subnet mask, therefore, must be selected before IP addresses can be assigned to devices on a subnetwork.

The following are the valid Class C subnet masks that can be used:

Class C Subnet Masks:

255.255.255.192
255.255.255.224
255.255.255.240
255.255.255.248
255.255.255.252

When a device is designed to permit subnetworking, and subnetworking is not used, the subnet mask for the device is configured to indicate a *network mask*, which is the same as *no mask*. The following are the *network mask* configurations for the subnet mask for each network size:

Network Class	Subnet Mask = No Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

B.3.2.2 Class C Subnetworking Using RIP 1

For the Class C subnetworking method described in this section, Table B-1 shows the following for each of the five valid Class C subnet masks:

- the number of subnetworks that are available
- the number of hosts that can be connected to each subnetwork
- valid subnetwork numbers that can be used with the selected subnet mask
- valid host numbers that can be used for each subnetwork number for the selected subnet mask

In a Class C network, the host number makes up the fourth octet of the IP address. The subnetwork number is not configured as part of the IP address. The device uses the subnet mask and the host number to calculate the subnetwork number.

Table B-1. Valid Class C Subnetworks (1 of 4)				
Valid Host Numbers				
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.128	1/2*	126	0*	1 – 126
			128	129 – 254
255.255.255.192	3/4*	62	0*	1 – 62
			64	65 – 126
			128	129 – 190
			192	193 – 254
255.255.255.224	7/8*	30	0*	1 – 31
			32	33 – 62
			64	65 – 94
			96	97 – 126
			128	129 – 158
			160	161 – 190
			192	193 – 222
			224	225 – 254
255.255.255.240	15/16*	14	0*	1 – 14
			16	17 – 30
			32	33 – 46
			48	49 – 62
			64	65 – 78
			80	81 – 94
			96	97 – 110
			112	113 – 126
			128	129 – 142
			144	145 – 158
			160	161 – 174
			176	177 – 190
			192	193 – 206
			208	209 – 222
			224	225 – 238
			240	241 – 254

* Only when Subnet Zero is enabled (see IP Global Configuration screen on page 5-40).

Table B-1. Valid Class C Subnetworks (2 of 4)				
Valid Subnetwork Numbers				Valid Host Numbers
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.248	31/32*	6	0*	1 – 6
			8	9 – 14
			16	17 – 22
			24	25 – 30
			32	33 – 38
			40	41 – 46
			48	49 – 54
			56	57 – 62
			64	65 – 70
			72	73 – 78
			80	81 – 86
			88	89 – 94
			96	97 – 102
			104	105 – 110
			112	113 – 118
			120	121 – 126
			128	129 – 134
			136	137 – 142
			144	145 – 150
			152	153 – 158
			160	161 – 166
			168	169 – 174
			176	177 – 182
			184	185 – 190
			192	193 – 198
			200	201 – 206
			208	209 – 214
			216	217 – 222
			224	225 – 230
			232	233 – 238
			240	241 – 246
			248	249 – 254

* Only when Subnet Zero is enabled (see IP Global Configuration screen on page 5-40).

Table B-1. Valid Class C Subnetworks (3 of 4)				
Valid Host Numbers				
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.252	63/64*	2	0*	1, 2
			4	5, 6
			8	9, 10
			12	13, 14
			16	17, 18
			20	21, 22
			24	25, 26
			28	29, 30
			32	33, 34
			36	37, 38
			40	41, 42
			44	45, 46
			48	49, 50
			52	53, 54
			56	57, 58
			60	61, 62
			64	65, 66
			68	69, 70
			72	73, 74
			76	77, 78
			80	81, 82
			84	85, 86
			88	89, 90
			92	93, 94
96	97, 98			
100	101, 102			
104	105, 106			
108	109, 110			
112	113, 114			
116	117, 118			
120	121, 122			
124	125, 126			

Table B-1. Valid Class C Subnetworks (4 of 4)				
Valid Host Numbers				
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.252	63/64*	2	128	129, 130
			132	133, 134
			136	137, 138
			140	141, 142
			144	145, 146
			148	149, 150
			152	153, 154
			156	157, 158
			160	161, 162
			164	165, 166
			168	169, 170
			172	173, 174
			176	177, 178
			180	181, 182
			184	185, 186
			188	189, 190
			192	193, 194
			196	197, 198
			200	201, 202
			204	205, 206
			208	209, 210
			212	213, 214
			216	217, 218
			220	221, 222
			224	225, 226
			228	229, 230
			232	233, 234
			236	237, 238
240	241, 242			
244	245, 246			
248	249, 250			
252	253, 254			

* Only when Subnet Zero is enabled (see IP Global Configuration screen on page 5-40).

Figure B-6 shows an example of Class C subnetworking using RIP 1. See page B-14 For an example of Class C subnetworking using unnumbered links.

In Figure B-6, the IP address assigned by the service provider is a Class C address. It can be recognized as a Class C address because the number in the first octet (192) is within the range for Class C networks (192 through 255).

Since seven subnetworks are required (four for the different sites and three for the links between sites) a subnet mask must be selected that permits at least seven subnetworks. The first subnet mask in Table B-1 that permits at least seven subnetworks is 255.255.255.224. This subnet mask permits up to seven subnetworks (8 when Subnet Zero is enabled) and up to 30 hosts on each subnetwork.

It is good practice when selecting subnetwork numbers to look at the subnetwork topology as a tree, and to assign the lowest subnetwork number at the top of the tree and increasingly higher numbers to the lower branches. For this reason, the first subnetwork number assigned in the figure is subnetwork 32. In Table B-1, it can be seen that hosts on subnetwork 32 for subnet mask 255.255.255.224 can be numbered 33 through 62 (details from Table B-1 for subnet mask 255.255.255.224 are reprinted on this page for convenient reference). If either of the three routers on subnetwork 32 receives information that is to be routed to any host with a host number of 33 through 62, the router uses the subnet mask to calculate that this host is located on subnetwork 32.

In Figure B-6, note the following:

- The IP address assigned to the interface noted in the figure as leading "To Internet" is not part of any of the subnetworks. This IP address is on the service provider's network, and has the service provider's network number.
- The single IP address assigned by the service provider to the customer is assigned to the first LAN interface from the top in the figure. Note that, for this IP address, only the network number is assigned by the service provider.

- Seven subnetworks are required. Four subnetworks (subnetworks 32, 128, 160, and 224) can contain hosts in addition to the router interfaces on each subnetwork. Three subnetworks (subnetworks 64, 96, and 192) are required to address the links for router interfaces between different subnetworks.
- All subnetworks in the example have the same network number (192.3.5.0), which is the network number assigned by the service provider.
- The subnetwork number is not configured in dotted decimal notation as part of the IP address, but is extrapolated from the subnet mask and the host number.
- Each interface for each router connects to a different subnetwork.
- Hosts on a LAN that is located between the interfaces of two connected routers would be on the same subnetwork as the two router interfaces (see subnetworks 32, 128, 160, and 224).

Example: Subnet Mask 255.255.255.224 (part of Table B-1)				
				Valid Host Numbers
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.224	7/8*	30	0*	1 – 31
			32	33 – 62
			64	65 – 94
			96	97 – 126
			128	129 – 158
			160	161 – 190
			192	193 – 222
			224	225 – 254

* Only when Subnet Zero is enabled.

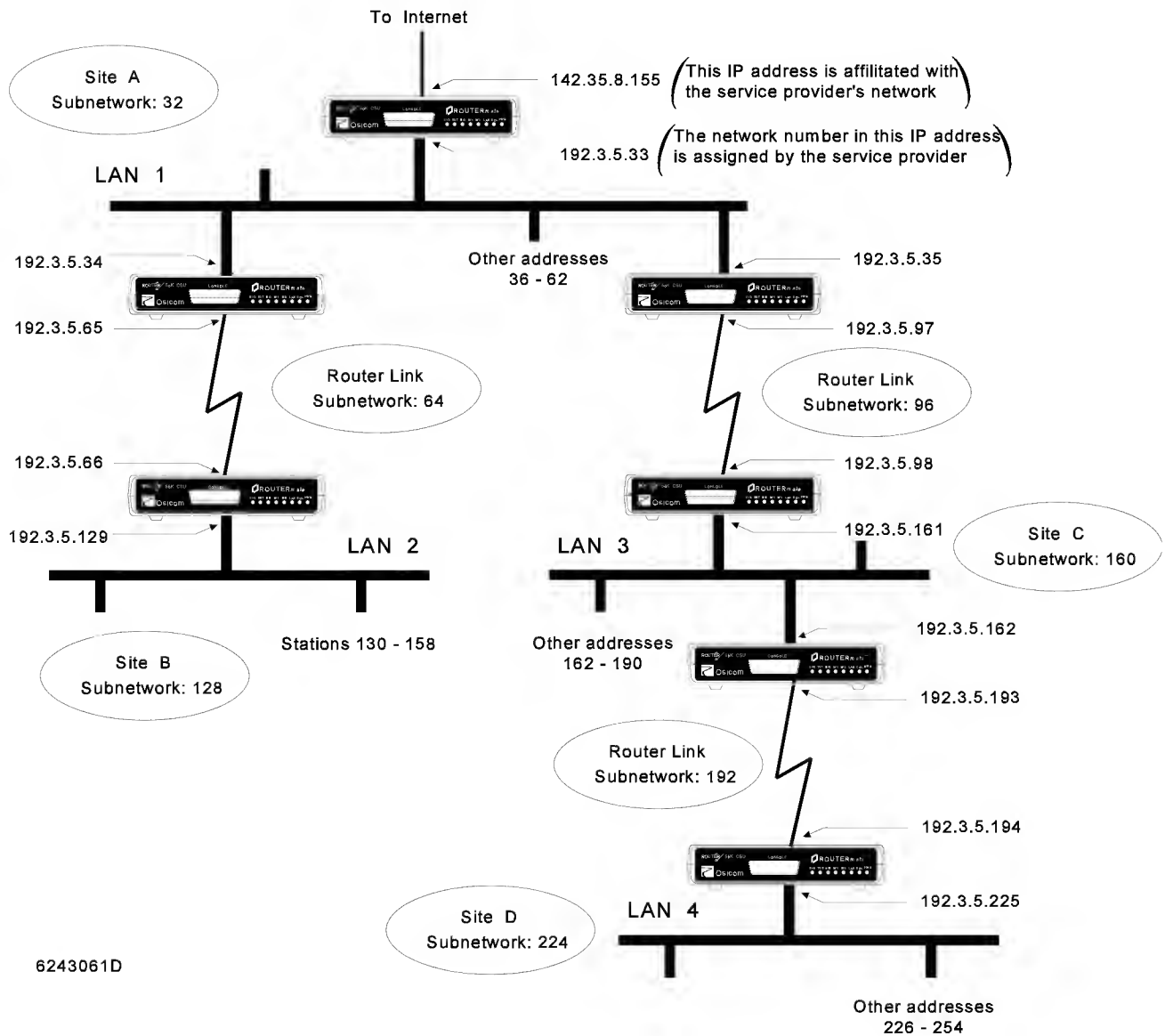


Figure B-6. Class C Subnetworking Example Using RIP 1

B.3.2.3 Class C Subnetworking Using Unnumbered WAN Links

Figure B-7 shows an example of Class C subnetworking using Unnumbered WAN links. See page B-12 for an example of Class C subnetworking using RIP 1.

In Figure B-7, the IP address assigned by the service provider is a Class C address. It can be recognized as a Class C address because the number in the first octet (192) is within the range for Class C networks (192 through 255).

Since four subnetworks are required (for LANs 1-4) a subnet mask must be selected that permits at least four subnetworks. The first subnet mask in Table B-1 that permits at least four subnetworks is 255.255.255.192. This subnet mask permits four subnetworks (when Subnet Zero is enabled). No addresses are required for the links between sites. Remember to consider future growth needs. Select the subnet that allows the maximum number of stations on each segment.

It is good practice when selecting subnetwork numbers to look at the subnetwork topology as a tree, and to assign the lowest subnetwork number at the top of the tree and increasingly higher numbers to the lower branches. For this reason, the first subnetwork number assigned in the figure is subnetwork 0. In Table B-1, it can be seen that hosts on subnetwork 0 for subnet mask 255.255.255.192 can be numbered 1 through 62 (details from Table B-1 for subnet mask 255.255.255.192 are reprinted on this page for convenient reference). If either of the three routers on subnetwork 0 receives information that is to be routed to any host with a host number of 1 through 62, the router uses the subnet mask to calculate that this host is located on subnetwork 0.

In Figure B-7, note the following:

- The IP address assigned to the interface noted in the figure as leading "To Internet" is not part of any of the subnetworks. This IP address is a numbered link on the service provider's network, and has the service provider's network number.

- The single IP address assigned by the service provider to the customer is assigned to the first LAN interface from the top in the figure. Note that, for this IP address, only the network number is assigned by the service provider.
- Four subnetworks are required. Four subnetworks (subnetworks 0, 64, 128, and 192) can contain hosts in addition to the router interfaces on each subnetwork. When running Unnumbered Links, no addresses or subnets are used by WAN interfaces.
- All subnetworks in the example have the same network number (192.3.5.0), which is the network number assigned by the service provider.
- The subnetwork number is not configured in dotted decimal notation as part of the IP address, but is extrapolated from the subnet mask and the host number.
- Each interface for each router connects to a different subnetwork.
- Hosts on a LAN that is located between the interfaces of two connected routers would be on the same subnetwork as the two router interfaces (see subnetworks 0, 64, 128, and 192).

Example: Subnet Mask 255.255.255.192 (part of Table B-1)				
Valid Subnetwork Numbers			Valid Host Numbers	
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.192	3/4*	62	0*	1 – 62
			64	65 – 126
			128	129 – 190
			192	193 – 254

* Only when Subnet Zero is enabled.

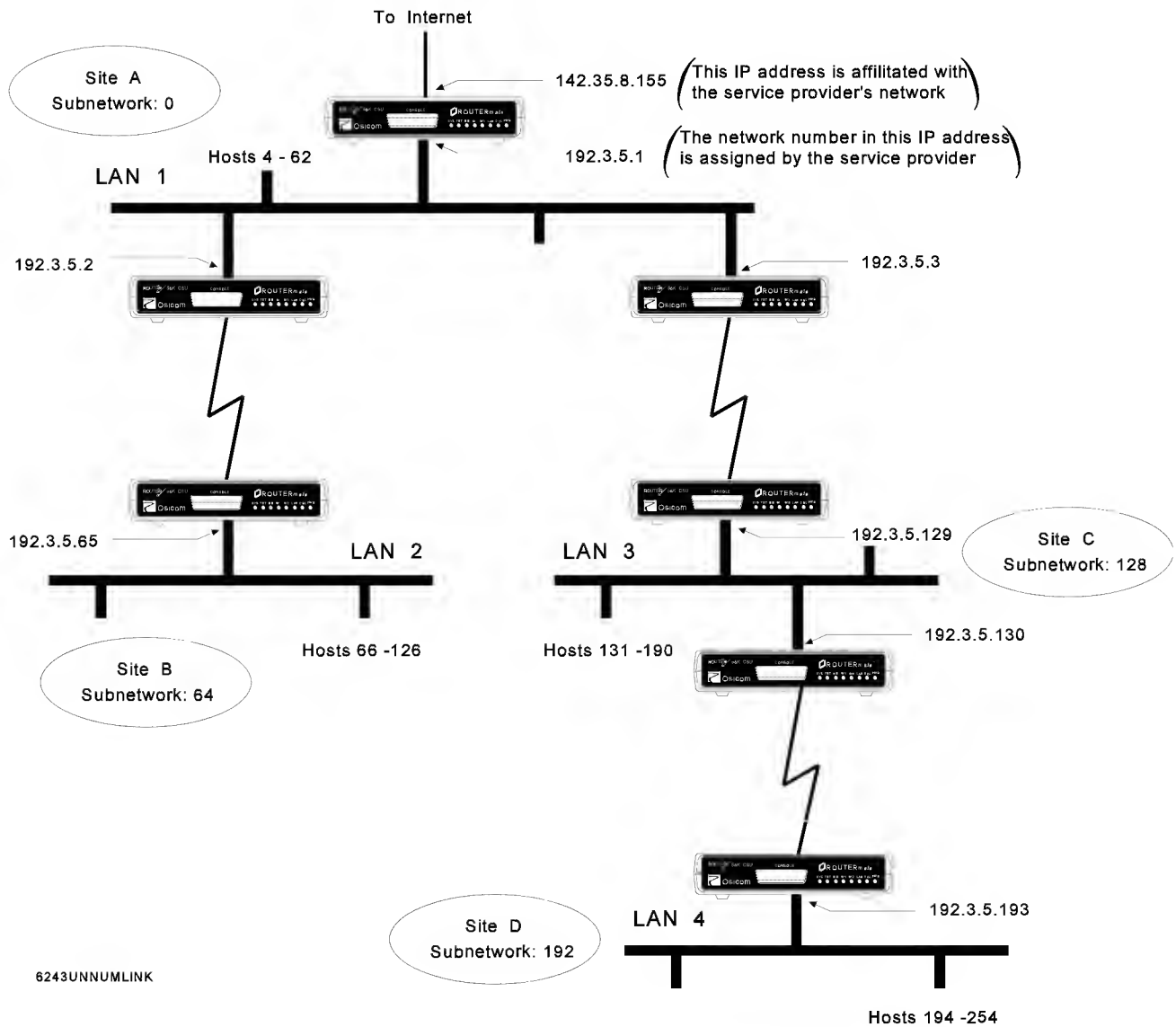


Figure B-7. Class C Subnetworking Example Using Unnumbered WAN Links

B.3.3 Address Resolution

The final communication to any host uses the host's physical hardware address, not the IP address. For an Ethernet LAN, the physical hardware address is the MAC address.

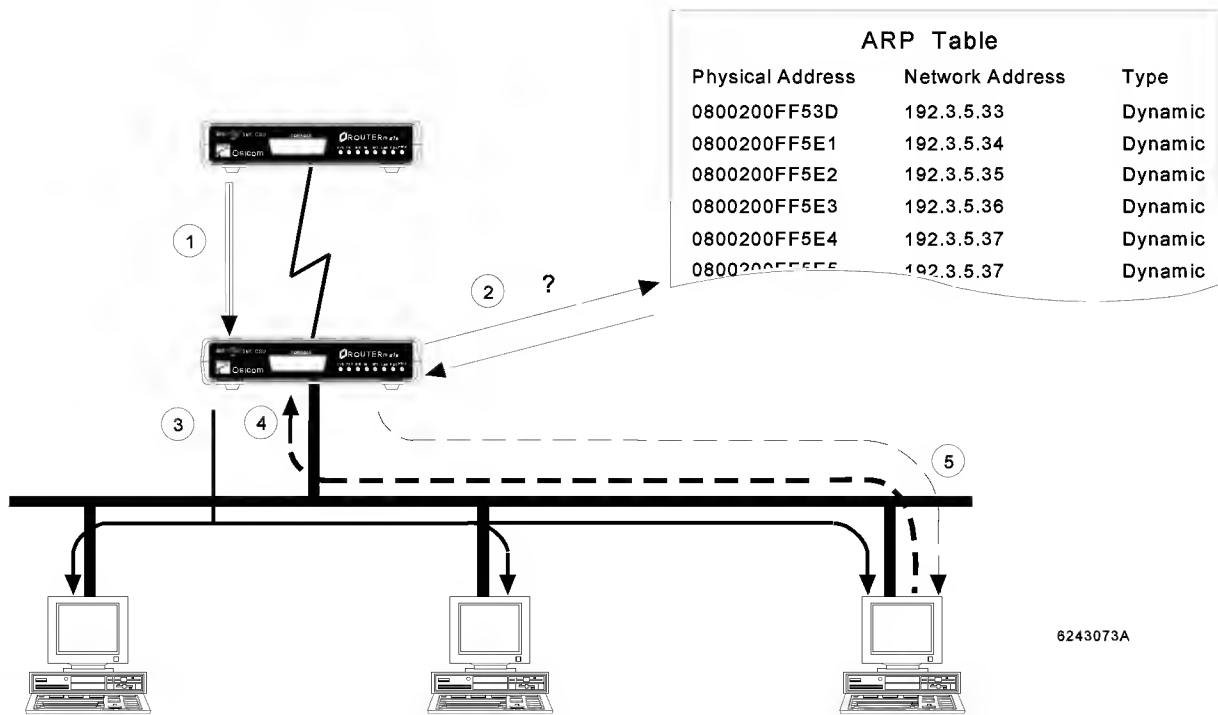
In the router, the MAC address of a host on the LAN is not permanently mapped to the device's IP address. Instead, the router uses the Address Resolution Protocol (ARP) to determine the MAC address. IP addresses and MAC addresses for devices with which the router has communicated recently are retained in the router's ARP table. By referring to the ARP table before broadcasting an ARP request, the router is required to send fewer ARP requests.

The process is shown in five steps in Figure B-8, as follows:

1. The local router receives an IP packet that contains an IP address for a local host.
2. The router checks its ARP table for a MAC address that is associated with the received IP address. If the MAC address is in the ARP table, the router routes the packet to the correct MAC address (Step 5.)
3. If the MAC address is not in the ARP table, the router broadcasts an ARP request to all local hosts. The request includes the IP address for which a MAC address is needed.
4. Only the host with the specified IP address replies. The unknown host sends a reply ARP packet that contains its MAC address.
5. The router then forwards the packet to the host.

All addresses in the ARP table are learned dynamically through ARP requests and replies. As the table grows, few ARP messages are required unless a new host is added or a device's Ethernet card is replaced.

The ARP table can contain approximately 2000 addresses.

**Figure B-8. Packet Delivery Using ARP**

B.3.4 RIP

Routers in an IP environment use the Routing Information Protocol (RIP) to exchange routing information.

A router maintains a routing table that contains routing information for the entire network topology and is used to inform other routers about the network topology.

Each router advertises only to its adjacent routers. RIP messages advertise the information in the routing table to adjacent routers, and request information from adjacent routers, as follows:

- Upon power-up, an initial broadcast informs adjacent routers of networks that can be reached through the router.
- Upon power-up, an initial broadcast requests that adjacent routers provide routing information.
- Periodic broadcasts inform adjacent routers of current routes.
- A network topology change triggers an update to adjacent routers of current routes.

The routing table lets the router:

- Locate the fastest route.
- Retrieve routing information from other routers.
- Respond to requesting routers.
- Advertise the latest internetwork configuration.
- Advertise internetwork topology changes.

If a router does not receive an update for a route after a specified time, the router deletes the route from its routing table, marks the route as unusable, and broadcasts the revised current table to adjacent routers.

RIP describes the distance between a router and a destination network in *hops*. A network immediately adjacent to the local router is 1 hop away, a network that is reached by passing through 2 routers is 2 hops away, and so on.

Each router sends RIP messages that advertise the paths to networks that can be reached via that router.

Information in the RIP messages includes, for each destination network, such routing information as the IP network number of the destination network, the number of hops to the network, and the *next hop* IP address (the address of the next router to which packets are sent).

Figure B-9 illustrates a single network (Network A) that consists of four LANs connected by routers; the network is organized into seven subnetwork (4 LANs plus 3 router links).

Subnetwork information is routed only within the subnetwork. In the figure, Router 1 advertises only Network A to the Internet, and advertises the Internet to routers connected to Subnet 1.

As seen in the figure, each router advertises only to its adjacent routers. For example, Router 5 advertises only to Routers 4 and 6.

Routers receiving the RIP messages update their routing tables accordingly and advertise to routers adjacent to them. The cumulative effect is that each router advertises to its neighbors all networks that can be reached through the router.

A path to a network (or subnetwork) that is learned over a particular interface is not advertised back over the same interface, since this would be redundant. For example, Router 2 advertises to Routers 1 and 4 only its paths to Subnets 2 and 3. To Router 3, however, Router 2 advertises its paths to the Internet and to Subnets 1, 4, 5, 6, and 7.

Devices other than routers can receive messages and use them to update their routing tables, but only routers advertise their routes.

Novell IPX networks also use a Routing Information Protocol. The RIP used by IP is different from the RIP used by IPX, although the purposes of both are similar.

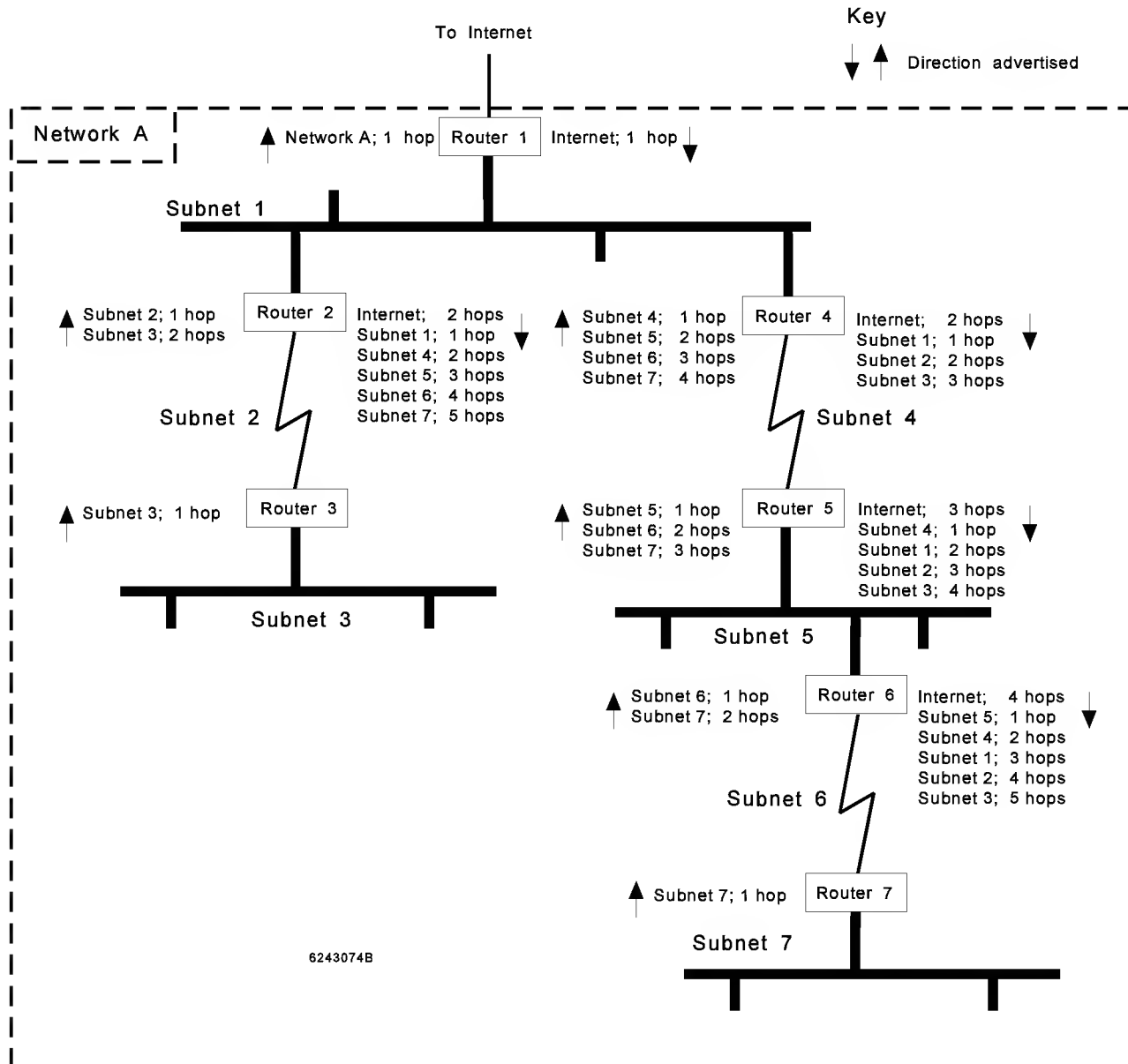


Figure B-9. RIP Advertising Example

B.3.5 Types of IP Routes

There are three types of IP routes:

- *Direct* - The source router is directly connected to the destination network.
- *Static* - A permanently-configured route.
- *RIP* - A route that is learned from a RIP update packet.

Default Route - A fourth type, a *default* route, is actually a static route that is permanently configured for a specific purpose: if a received packet is destined for a network that is not listed in the router's routing table, the packet can be forwarded to a default route.

Direct and Learned Routes - Figure B-10 illustrates directly-connected and learned routes.

In the figure, the path between Router 1 and Router 2 is direct, and the path between Router 2 and Router 3 is direct. Routers 1 and 3 can learn about each other only by receiving RIP update packets from Router 2, so the paths between Routers 1 and 3 are learned.

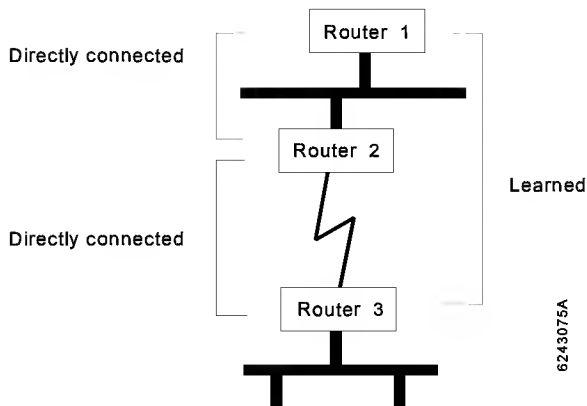


Figure B-10. Direct and Learned Routes

Static Routes - A static route can be created when the router cannot dynamically build a route to the destination, or when it is desirable to reduce traffic over a slow, expensive link.

In Figure B-11, a remote device connected over a WAN link is being booted through the router. A static route must be assigned to the network of the device being booted.

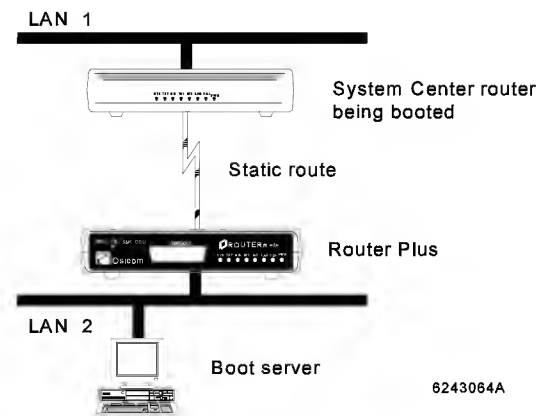
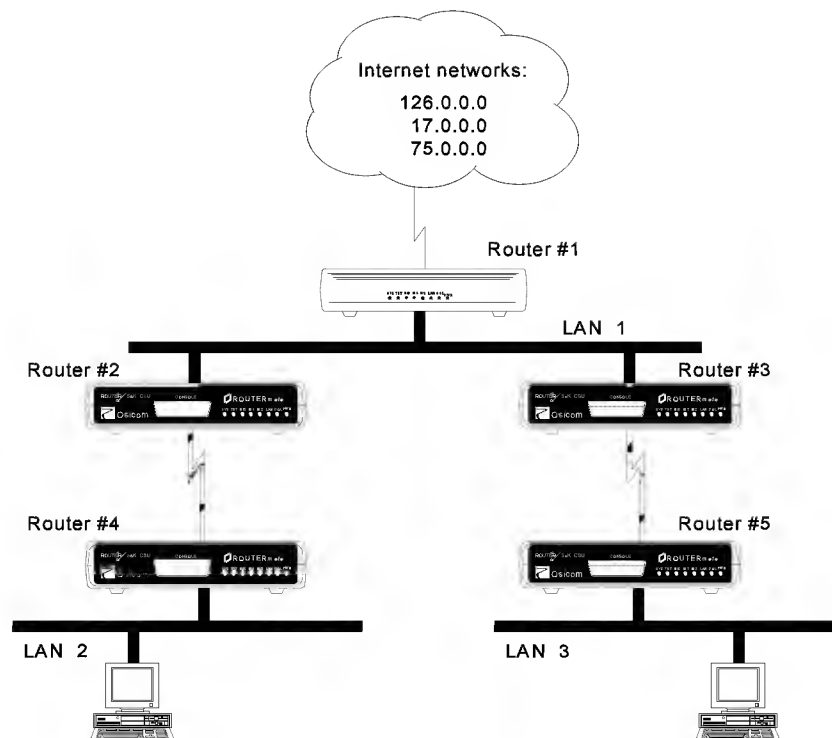


Figure B-11. Static Route to a Remotely-Booted Device

In Figure B-12, LAN 2 and LAN 3 wish to connect to internet networks 126.0.0.0, 17.0.0.0, and 75.0.0.0, but Router 1 does not run RIP.

A static route must be created for routers 2 and 3 to networks 126.0.0.0, 17.0.0.0, and 75.0.0.0. Routers 2 and 3 will then use RIP to announce these static routes, which will let routers 4 and 5 know that the routes are available. LANs 2 and 3 can then reach the three networks.

A static route is floating. That is, if another route with a lower metric is available to the destination, the route with the lowest metric is taken. The metric for a static route is assigned a value of 1 by default and can be re-configured for a value of 1 through 15.



6243065A

Figure B-12. Static Route to a non-RIP Router

B.3.6 IP Filtering

IP traffic can be filtered to keep certain types of routing information from being received or advertised.

For example, this might be done to:

- restrict access between certain networks
- reduce the amount of routing information traffic (a particularly desirable feature when communicating over packet switched networks)

Ways in which a router might be configured to filter IP traffic could include such filtering as the following:

- Disabling the announcement of static routes, and the default route.
- Receiving (listening to) RIP update messages, but not advertising its own routes.
- When subnetworking is used, a router can (and typically should) be set to advertise only the parent network address of IP subnetworks to other IP networks.
- Specifying addresses from which RIP update packets will or will not be accepted.
- Specifying addresses to which RIP update packets will or will not be sent.

B.4 IPX Routing

The most common type of LAN management software is Novell's NetWare. Novell uses an Internetwork Packet Exchange (IPX) protocol for LAN communications. IPX defines addressing schemes for internetwork and intra-node communications.

Novell IPX routing is based upon IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP).

Novell IPX calculates the best route to a destination based upon routing time delays associated with the links and with the number of hops (intermediate routers) taken to reach a network.

Novell IPX RIP is not the same as IP RIP, although the purposes of both are similar.

B.4.1 Frame Types

A router must be configured to recognize which of several IPX frame types is used on the Novell LAN.

Figure B-13 illustrates several IPX frame types:

Ethernet 802.2 (RAW)
 Ethernet 802.3 (LLC)
 Ethernet Type II
 Ethernet SNAP

Except for the IPX Frame Header, each type of IPX frame is composed of a consistent number of fields and bytes. However, for each IPX frame type the IPX Frame Header varies in the number of bytes and the number of fields in the header.

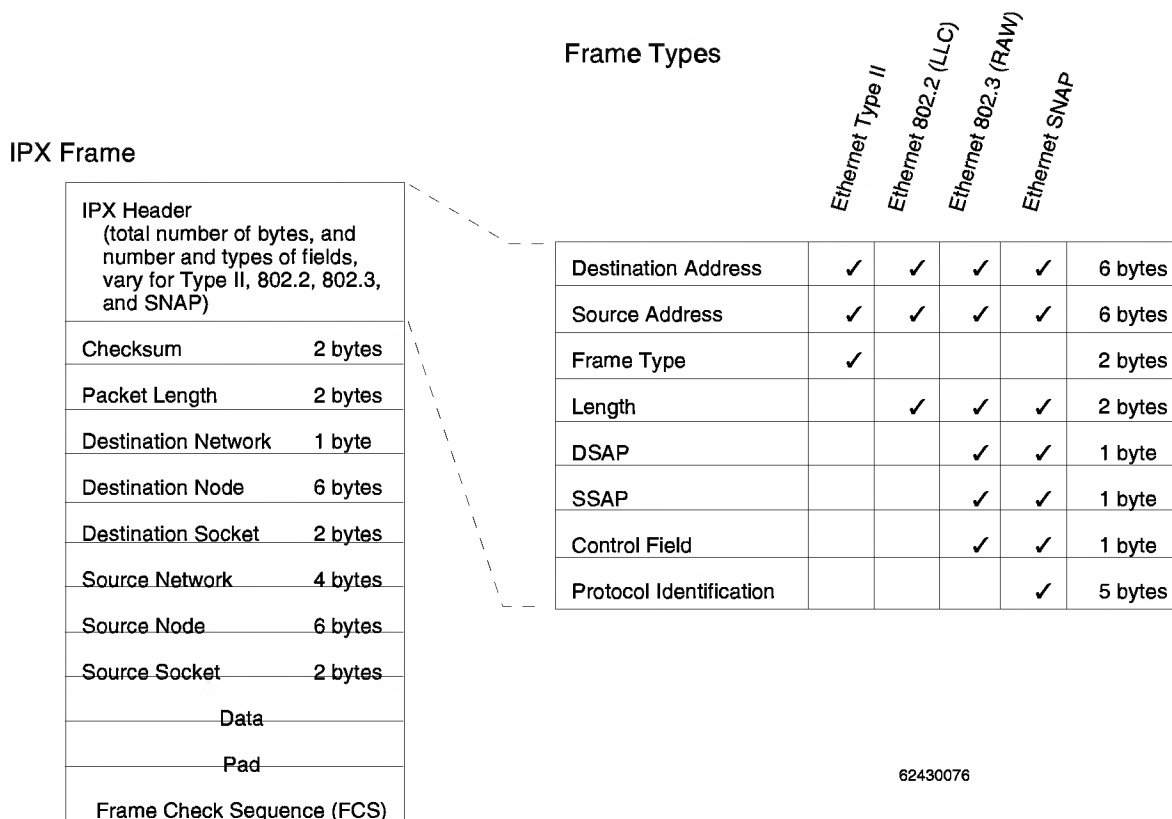


Figure B-13. IPX Frame Types

B.4.2 Novell Addressing

A Novell IPX address is written in hexadecimal notation. It consists of a 4-byte network number, followed by a 6-byte node ID, and a 2-byte socket number.

For example:

00000001 000080123403:0451.

The numbers in the example are:

Network number: 00000001
Node ID: 000080123403
Socket number: 0451

Network Number: A globally unique network number is assigned to each network interface of a Novell server. Servers and router interfaces attached to the same physical network must be configured with the same network number. To simplify network management, only servers and routers must be configured with a network number; workstation's network numbers are assigned automatically by the server (connection to local server) or router (connection to remote server).

Node ID: The Node ID is the MAC address for the device. It is incorporated automatically by software into the IPX address.

Reserved Socket numbers: The following sockets are reserved by Novell:

File Servers:

Socket	Description
451h	NCP process

Routers:

Socket	Description
452h	SAP process
453h	RIP process

Workstations:

Socket	Description
455h	Novell NetBIOS Process
456h	Diagnostics process
4000h to 7FFFh	Dynamically assigned sockets used by workstations for interaction with file servers and other network equipment
8000h to FFFFh	Other sockets assigned by Novell

NCP=Netware Core Protocol
SAP=Service Advertising Protocol
RIP=Routing Information Protocol

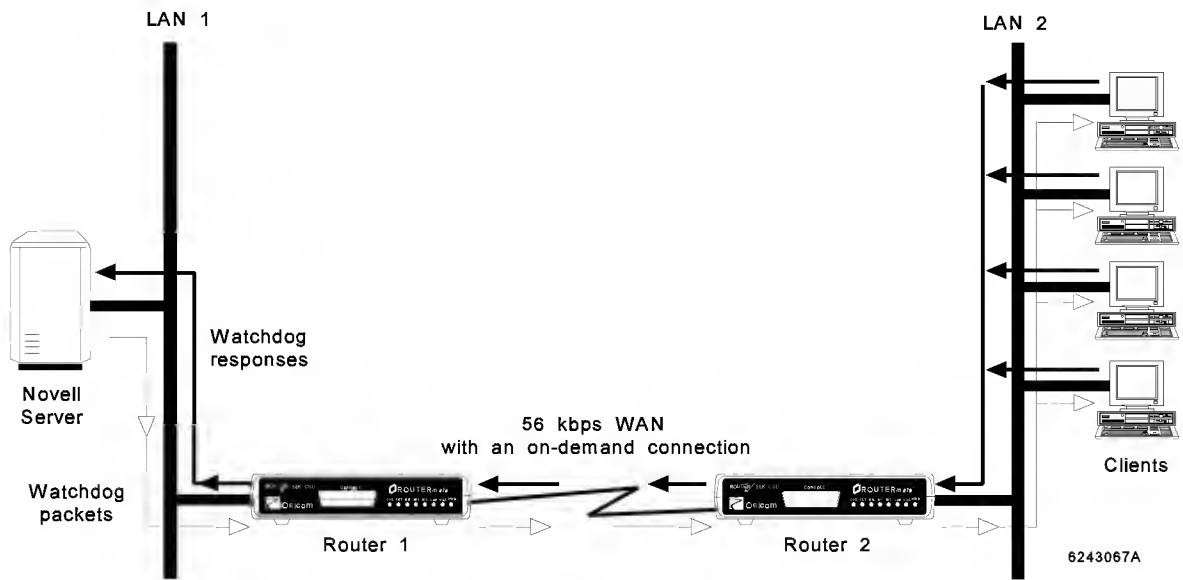
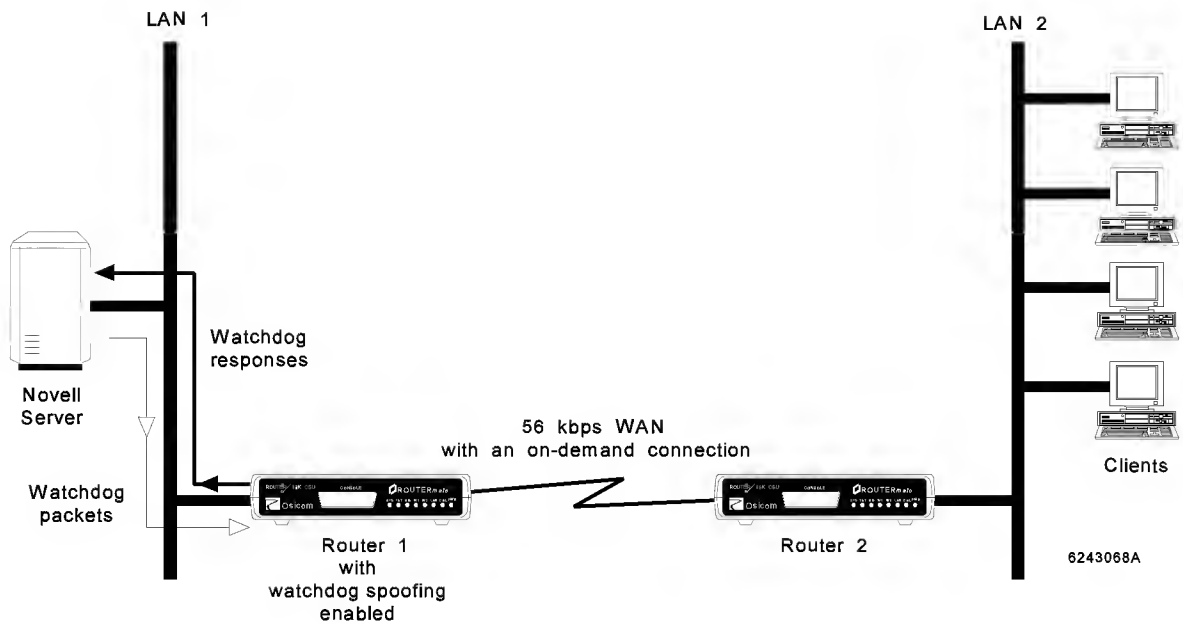
B.4.3 Watchdog Spoofing

A Novell file server keeps a table of when client sessions are established and terminated.

When a client has not communicated with a server in a pre-defined time, the server sends a *watchdog packet* to the client to ask if the client still is connected. If a client fails to respond to a pre-defined number of watchdog packets, the session is terminated at the server.

When communication between a number of clients and a server is over an on-demand WAN link, the link never gets a chance to be inactive, and operating costs are high (Figure B-14). Also, if the WAN link is brought down for some other reason, the client sessions might be terminated prematurely.

To counteract the problem of sending watchdog packets over on-demand WAN links, watchdog spoofing can be enabled for the router situated before the WAN link on the server's side (Figure B-15). The router then answers watchdog packets on behalf of clients. This prevents the WAN link from being activated just to send watchdog packets to clients.

**Figure B-14. Watchdog Spoofing Disabled****Figure B-15. Watchdog Spoofing Enabled**

B.4.4 RIP

Routers in an IPX environment use the IPX Routing Information Protocol (RIP) to exchange routing information. The RIP used by IPX is different from the RIP used by IP, although the purposes of both are similar.

A router maintains a routing table that contains routing information for the entire network topology and is used to inform other routers about the network topology.

Each router advertises only to its adjacent routers. RIP messages advertise the information in the routing table to adjacent routers, and request information from adjacent routers, as follows:

- Upon power-up, an initial broadcast informs adjacent routers of networks that can be reached through the router.
- Upon power-up, an initial broadcast requests that adjacent routers provide routing information.
- Periodic broadcasts inform adjacent routers of current routes.
- A network topology change triggers an update to adjacent routers of current routes.

The routing table lets the router:

- Locate the fastest route.
- Retrieve routing information from other routers.
- Respond to requesting routers.
- Advertise the latest internetwork configuration.
- Advertise internetwork topology changes.

RIP defines the distance between a router and a destination network in *hops*. A network immediately adjacent to the local router is 1 hop away, a network that is reached by passing through 2 routers is 2 hops away, and so on.

IPX RIP also applies a *time tick* value to each route to rate the time required to pass data over the route. Specifically, there are 18.21 time ticks in a second, so a time tick equals approximately 1/18 second. If a router has two routes to the same network, the router selects the route with the lowest time tick value. If the time ticks are the same, the router selects the route with the lowest hop count. If the hop counts are the same, the router selects either of the two routes.

In Figure B-16, a data packet is sent from LAN 1 to LAN 4 via LAN 2 and LAN 3 even though the selected LAN path is 3 hops and the WAN path is only 1 hop; the LAN path is selected because the transmission time of 3 ticks for this path is less than the transmission time of 4 ticks over the link with a speed of 56 kbps (transmission speed on Ethernet=10 Mbps).

Each router sends RIP update packets that advertise the networks that can be reached via that router. The RIP update packets contain, for each network that can be reached via the advertising router, the IPX network number, the number of hops to the network, and the number of time ticks to the network.

Routers receiving the RIP messages update their routing tables accordingly and advertise to routers adjacent to them. The cumulative effect is that each router advertises to its neighbors all networks that can be reached through the router.

A path to a network that is learned over a particular interface is not advertised back over the same interface, since this would be redundant and could result in routing loops.

Devices other than routers can receive RIP messages and use them to update their routing tables, but only routers advertise their routes.

If a router does not receive an update from an adjacent router for by a pre-determined time, the router marks the routes served by the adjacent router as unusable and broadcasts the revised current table to adjacent routers. If an additional pre-determined time elapses and the route still has not been updated, it is deleted from the router's routing table.

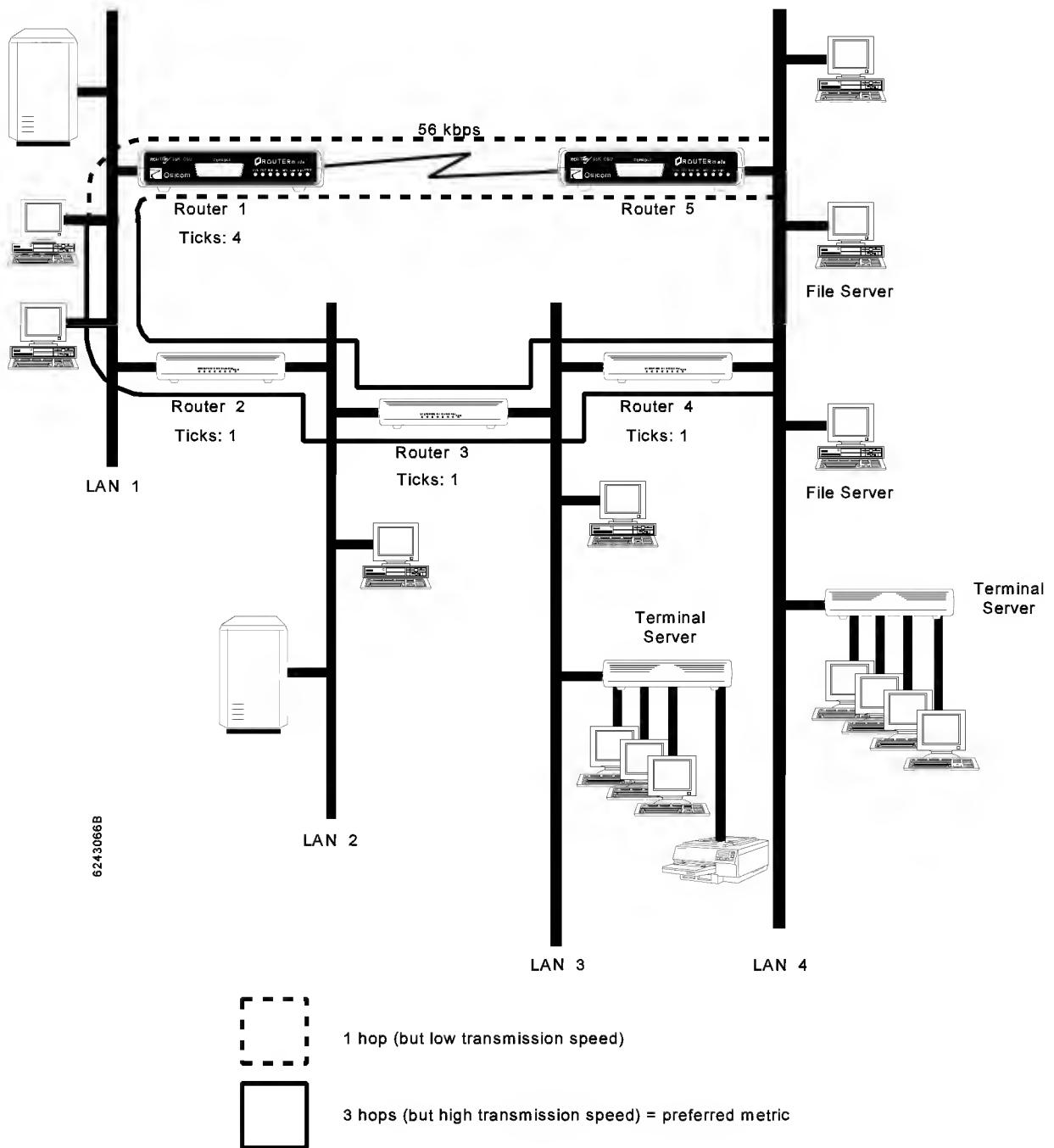


Figure B-16. IPX Transmission Over Fastest Path

B.4.5 RIP Filtering

IPX traffic can be filtered to keep certain types of routing information from being received or advertised.

For example, this might be done to:

- restrict access between certain networks.
- reduce the amount of routing information traffic (a particularly desirable feature when communicating over packet switched networks)

Ways in which a router might be configured to filter IPX traffic could include such filtering as the following:

- Specifying addresses from which RIP update packets will or will not be accepted.
- Specifying addresses to which RIP update packets will or will not be sent.

B.4.6 SAP

The Service Advertising Protocol (SAP) lets IPX devices advertise various Novell application services offered by such devices as file servers (file transfer), printer servers (print service) and gateways (protocol conversion).

A router has a SAP agent, which operates much like RIP. SAP agents collect and exchange service information about all the services available on the local network.

Table B-2 lists several commonly-used services.

Table B-2. Selected IPX Services	
SERVICE	SERVICE TYPE (OBJECT)
User	1
User Group	2
Print Queue	3
File Server	4
Job Server	5
Gateway	6
Print Server	7
Archive Queue	8
Archive Server	9
Job Queue	A
Administration	B
Remote Bridge Server 2	24
Bridge Server	26
TCP/IP Gateway	27
Archive Server SAP	2e
Advertising Print Server	47
Print Queue user	53
HP Laserjet	30c
Wildcard	FFFF

Workstations that require information about available services broadcast a SAP packet. For example, a workstation might broadcast "get nearest server;" the local SAP agent then responds with information about the nearest available file server.

SAP broadcasts are local broadcasts. They are initiated by servers once a minute and are received only by local SAP agents (i.e., the packets are not forwarded beyond the local segments).

SAP agents provide the following:

- Initiate workstation requests to get information about the name and address of the nearest server of a certain kind.
- Initiate router requests to get information about the names and addresses either of all servers, or of all servers of a certain kind on the internetwork.
- Send responses to requests originating from either a router or a workstation.
- Initiate periodic broadcasts by servers and routers.
- Update the accessible server information.

As with RIP routing, SAP routing keeps track of server addresses and the number of hops to the network on which the server is located. When a service is requested, it is routed along the fastest route.

Also, as with RIP, a SAP service is not advertised on the same port on which it was received since this would lead to redundancy.

B.4.7 SAP Filtering

Service information can be filtered to:

- Restrict access to servers by certain networks
- Reduce the amount of service information traffic (a particularly desirable feature when communicating over a low-speed WAN link)

Specifically, a router might advertise or accept SAP update packets according to network address, MAC address, service type, or a combination of these.

Table C-1. Console Interface

PIN	SIGNAL	DIRECTION
2	Transmit Data	Input
3	Receive Data	Output
5	Clear to Send	Output
6	Data Set Ready	Output
7	Signal Ground	—
8	Carrier Detect	Output



Table C-3. LAN Interface (10BaseT)

PIN	SIGNAL
1	Transmit Data (+)
2	Transmit Data (—)
3	Receive Data (+)
4	—
5	—
6	Receive Data (—)
7	—
8	—

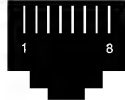


Table C-2. WAN 1 Interface

PIN	SIGNAL	DIRECTION
1	Transmit	Output
2	Transmit	Output
3	—	—
4	—	—
5	—	—
6	—	—
7	Receive	Input
8	Receive	Input

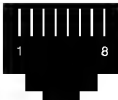


Table C-4. WAN 2 Interface (V.32 Modem)

PIN	SIGNAL
1	—
2	—
3	—
4	T Tip
5	R Ring
6	—
7	—
8	—



Table C-5. Router Cables		
DESCRIPTION	PART NUMBER	ORDER NUMBER
WAN 1 cable (included with unit)	115-0414-004	CBE04144 (7 ft)
DDD line cable (included with WAN 2 integral V.32 dial modem option)	115-0414-001	CBE04141 (7 ft)

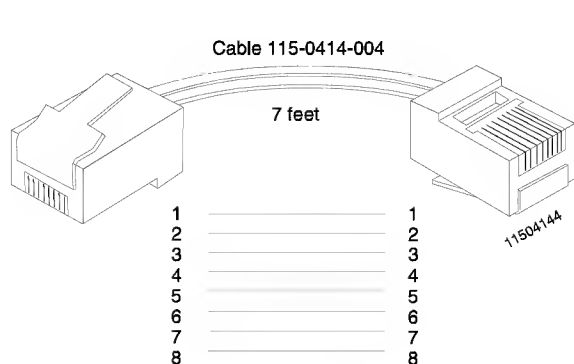
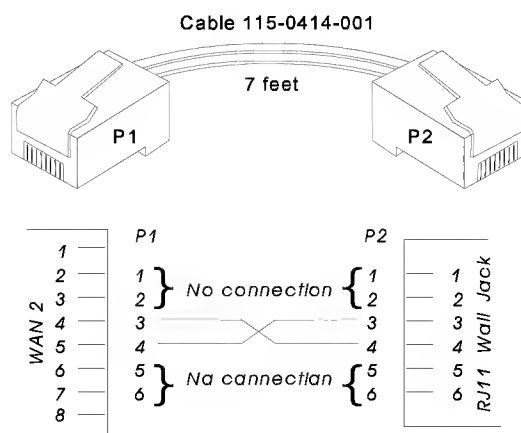


Figure C-1. WAN 1 Cable



NOTE: Cable 115-0414-001 is a 6-pin modular cable that connects the 8-pin WAN 2 interface to a 6-pin RJ11 wall jack. Cable connectors 3 and 4 connect to WAN 2 connectors 4 and 5, respectively.

Figure C-2. DDD Line Cable

Table D-1. Ordering Information	
DESCRIPTION	ORDER NUMBER
ROUTERmate Plus 56 (Router plus 56K CSU) IP and IPX router with bridging and integral 56K CSU; one 10Base-T LAN interface; one 56 kbps WAN interface (WAN 1); 7-foot RJ48S line cable; wall-mount power transformer. Console, SNMP, and Telnet manageable. Includes base software, 1 MB RAM and 1 MB flash PROM.	R56
Rackmount card version of above model.	R56R
Order the options listed below by adding the order number to the base model order number. Example: R56/B1/D1/E1 WAN 2 - Integral V.32 management modem; used for dial-in terminal management from a remote location. Includes 7-foot DDD line cable (115-0414-001). 4 MB SIMM memory module; increases unit's RAM to 4 MB total. Standard DES hardware encryption; used to add payload encryption on links of 56k for PPP or Frame Relay; compatible with FPX4802/DES Frame Relay Encryptor.	B1 D1 E1
Management Enterprise MIB written in standard ASN.1 notation. OsicomView network management for Windows. Contains Castle Rock's SNMPc management software plus BitView graphical user interface applications for Osicom's Internetworking products (3.5" DOS formatted disks). BitView graphical user interface (applications only).	Free download from Osicom's Web site at http://www.osicom.com OsicomView OsicomView/Apps
Power Wall-mount transformer (spare for standalone unit)	550-0366-02

Table D-1. Ordering Information	
DESCRIPTION	ORDER NUMBER
MiniRack	
6-slot rack for ROUTERmate product family of routers and CSU/DSUs	RM-MiniRack
6-slot rack for ROUTERmate product family of routers and CSU/DSUs; includes 115 VAC power transformer and mounting brackets	RM-MiniRack/115
6-slot rack for ROUTERmate product family of routers and CSU/DSUs; includes redundant -48 VDC power supply and mounting brackets	RM-MiniRack/48V
115 VAC power transformer (spare)	905-7593-01
115 VAC power transformer rack mounting kit	415-0043-01
-48 VDC power module (spare)	905-7287-03
DES Master Key License	
Only one needed per network. For encryption option (E1); lets network administrator re-program, via terminal, both the master key and initial vector. License application provided to the customer at time of order.	DES-KEY-LIC
Manual	
Routermate Router Plus 56K CSU Installation and Operation.	918-6243

Table E-1. Routermate Plus 56K CSU Specifications (1 of 2)

ITEM	DESCRIPTION
Protocol Support	
Routing	IP, IPX/SPX, RIP (IP), RIP/SAP (IPX/SPX)
Bridging	All popular LAN protocols, transparent bridging
LAN frame types	Type II, 802.2 (LLC), 802.3 (RAW), SNAP
WAN 1 frame types	Frame relay, point-to-point (PPP)
Interfaces	
LAN	Ethernet 10BaseT (RJ45)
WAN 1	Integral 56K CSU
Speed (NI)	56 kbps (RJ-48S)
Timing	Internal or Repeater
Diagnostics	V.54 w/integral 511 test generator
WAN 2 (optional)	Integral management modem
Speed (NI)	V.32 (RJ11)
Management	
Console	Asynchronous via RS-232
Speed (DCE)	9600 bps (DB25)
Telnet	Built-in default IP address (user configurable)
BootP	Configuration to Flash
TFTP (Client)	Operating system and configuration to Flash
SNMP	Enterprise MIB, MIB II, and Encryption MIB (Get, Set, Trap)
Integral Modem (optional)	V.32 (RJ11)
Graphical User Interface (optional)	Castle Rock <i>SNMPc</i>
Security (optional)	Integral DES Encryptor module
Memory	
1 MB RAM	SIMM upgrade to 4 MB
1 MB Flash PROM	Pre-loaded with router OS software
RFC Compliance	768, 791, 792, 793, 826, 854, 855, 862, 894, 903, 919, 922, 950, 951, 1010, 1058, 1155, 1157, 1166, 1212, 1213, 1315, 1332, 1350, 1490, 1542, 1552, 1570, 1634, 1638, 1661, 1723

Table E-1. Routermate Plus 56K CSU Specifications (2 of 2)

ITEM	DESCRIPTION
Power	
Standalone	Input: 120 VAC, 60 Hz; Output: 9 VAC @ 1 amp Input: 120 VAC, 60 Hz; Output: 9 VAC @ 2.1 amps (for units with optional encryption, compression, and WAN 2 interface installed)
6-slot MiniRack	AC module: Input: 120 VAC, 60 Hz; Output: 10 VAC @ 10 A DC module: Input: -48 VDC @ 6.25 A; Output: 8 to 12 VAC (9.5 nominal) @ 21.6 A max.
Dimensions	
Standalone	6.25" W x 9.6" D x 1.6" H
6-slot rack	17" W x 10.5" D x 3.5" (2U) H
Weight	
Standalone	2.3 lbs. fully-loaded (includes transformer)
Rack-mount card	1.4 lbs. (includes front and rear panels)
6-slot rack	7.7 lbs. empty (includes transformer)
Operating Temperature	32° to 104° F, 0° to 40° C
Relative Humidity	0% to 95%, non-condensing

4800 SERIES ROUTER_{mate}[™]		905-7591-	179-0512-01 REV C																					
FOR 120VAC POWER USE PWR MOD 905-7593-01 120VAC 60Hz 1A	FOR 48VDC POWER USE PWR MOD 905-7598-01 48VDC 6.25A	Complies with Part 68 FCC Rules when used with the following registered equipment :																						
BARCODE LABEL		<table border="1"> <thead> <tr> <th>Product</th> <th>Registration No.</th> <th>Ringer Equivalence</th> </tr> </thead> <tbody> <tr> <td>T1 CSU/DSU</td> <td>1R5USA-23055-DE-N</td> <td>N/A</td> </tr> <tr> <td>56K CSU/DSU</td> <td>1R5USA-23056-DE-N</td> <td>N/A</td> </tr> <tr> <td>T1 DROP & INSERT</td> <td>1R5USA-31067-DE-N</td> <td>N/A</td> </tr> <tr> <td>ROUTER plus T1 CSU</td> <td>1R5USA-24168-DE-N</td> <td>N/A</td> </tr> <tr> <td>ROUTER plus 56K CSU</td> <td>1R5USA-24165-DE-N</td> <td>N/A</td> </tr> <tr> <td>V.32 MODEM</td> <td>1R5USA-24168-DE-N</td> <td>N/A</td> </tr> </tbody> </table>		Product	Registration No.	Ringer Equivalence	T1 CSU/DSU	1R5USA-23055-DE-N	N/A	56K CSU/DSU	1R5USA-23056-DE-N	N/A	T1 DROP & INSERT	1R5USA-31067-DE-N	N/A	ROUTER plus T1 CSU	1R5USA-24168-DE-N	N/A	ROUTER plus 56K CSU	1R5USA-24165-DE-N	N/A	V.32 MODEM	1R5USA-24168-DE-N	N/A
		Product	Registration No.	Ringer Equivalence																				
T1 CSU/DSU	1R5USA-23055-DE-N	N/A																						
56K CSU/DSU	1R5USA-23056-DE-N	N/A																						
T1 DROP & INSERT	1R5USA-31067-DE-N	N/A																						
ROUTER plus T1 CSU	1R5USA-24168-DE-N	N/A																						
ROUTER plus 56K CSU	1R5USA-24165-DE-N	N/A																						
V.32 MODEM	1R5USA-24168-DE-N	N/A																						
AFFIX LABEL HERE	AFFIX LABEL HERE	This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions : (1) This device may not cause harmful interference and (2) this device must accept any interference that may cause undesired operation.																						
MANUFACTURED BY  9020 Junction Drive Annapolis Junction, MD 20701-1104, U.S.A.		For T1 CSU/DSU : This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Pour T1 CSU/DSU : Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel du Canada.																						
http://www.osicom.com e-mail: info@osicom.com		FOR USE IN A RESTRICTED ACCESS LOCATION																						

Figure F-2. Multipurpose Label - MiniRack

NOTE

When the unit is powered up, a prompt appears on the screen, as shown in Figure G-1. To enter the diagnostics, press **D** within 3 seconds. The Diagnostic Menu (Figure G-2) is displayed.

Reproductive and Diagnostic
Control Technologies
Biomediagnostics

Figure G-1. Diagnostic Menu Prompt

```

Rebooting...
A-Defragment
B-RAM
C-Init
D-PS2 Download
E-System Information
X-Exit

Select [X]:

```

Figure G-2. Diagnostic Menu

G.1	LED Test	G-2
G.2	RAM Test	G-2
G.3	Flash Test	G-3
G.4	TFTP Software Download ...	G-4
G.5	System Information	G-5

G.1 LED Test

The LED test checks the operation of the TST, ALM, W1, W2, and LAN LEDs. The LEDs will go ON and OFF in sequence for 5 to 6 seconds.

ROUTERmate Plus 56k CSU Diagnostics

- ```
A - LED Test
B - RAM
C - Flash Test
D - TFTP Software Download
E - System Information
X - Exit
```

Select [A..E,X]: A

## TESTING LEDS

### Figure G-3. LED Test

## G.2 RAM Test

Test A executes a minimal verification of RAM that non-destructively tests the read-write functions of the RAM. The test returns a result of Passed or Failed.

Tests **B**, **C**, and **D** execute a thorough verification of RAM. These tests overwrite RAM. The user is then prompted to press a key, after which the unit will reboot.

If the test is successful, the following message appears:

RAM Test Passed

## RAM Tests

- ```
A - Non-destructive RAM Test
B - 32-bit destructive RAM Test - Auto reboot
C - 16-bit destructive RAM Test - Auto reboot
D - 8-bit destructive RAM Test - Auto reboot
X - Exit
```

Select [A..D,X]: A

Testing RAM - Please Wait

RAM Test Passed
Press any key to continue:

Figure G-4. RAM Test

If the test fails, the message below appears:

RAM Test Failed : Address = 0xnnnnnnnnn
(hex address)

G.3 Flash Test

Select **A** to view information about the flash memory, as shown in Figure G-5.

```
Flash Tests

A - Flash Info
B - Erase Configuration Flash
X - Exit

Select [A..B,X]: A

Program Flash Information:

Make/Model  = AMD 29F040
Bus Width   = 16 bits
Flash Width  = 16 bits
Sector Size  = 128K
Total Size   = 1024K

Press any key to continue:
```

Figure G-5. Flash Test - Flash Info

Select **B** to remove the configuration in flash.

At the 'Enter password' prompt, enter the console password as it was configured on the Unit menu (Chapter 8). The configuration flash will not be erased unless the correct password is entered.

The unit returns to the Flash Tests screen. When the software is run, the unit uses the default configuration.

```
Flash Tests

A - Flash Info
B - Erase Configuration Flash
X - Exit

Select [A..B,X]: B

Enter password:
```

Figure G-6. Flash Test - Erase Configuration Flash

G.4 TFTP Software Download

When you select TFTP Software Download, the screen shown in Figure G-7 appears. Use this option to download the router's operating software or boot software from a specified TFTP server via the router's LAN interface.

The commands are intended for error recovery when the full software image will not run. The user can also upgrade the boot code via this screen.

Software downloads can only be performed across the LAN because the WAN is not operational when running from the boot sector.

NOTE

You can download through another router on the local LAN if you configure the LAN address of the other router as the Gateway Address.

When this screen is initially entered, the data displayed will be whatever was configured in the database.

You can configure the LAN IP Address, Subnet Mask, Server Address, Filename, and Gateway Address manually or via BootP. If you choose the latter, the new values will be displayed once the BootP reply is received.

Manually configure the LAN type for either TYPE II or SNAP.

Selecting **Initiate BOOTP** does not cause the download to start. After you are satisfied that all fields are set properly, press **[G]** to start a download of the operating software or **[H]** to start a download of the boot software.

NOTE

Any changes to the fields on the TFTP Download screen do not change the database in the main operating software.

Router Plus 56k CSU Code Download

- A - Initiate BOOTP
- B - Configure Lan IP Address: 128.1.128.1
- C - Configure Lan IP Subnet Mask: 255.255.255.0
- D - Configure Server Address: 125.0.0.103
- E - Configure Filename: routerplus.txt
- F - Configure Gateway Address: 0.0.0.0
- G - Download Operational Code
- H - Download Boot Code
- I - Lan Frame Type: TYPE II
- X - Exit

Select [A..I,X]:

Figure G-7. TFTP Software Download

G.5 System Information

Select System Information to view details of the unit's internal software and hardware components, as shown in Figure G-8.

If encryption is installed, the version will be displayed.

NOTE

The contents of the System Information screen is an example; your screen contents will be different.

System Information:

MAC address = 00:00:6d:13:57:90
Boot code version = 2.x.xx
Software size = 607K
Software checksum = 0xcf777318
DB version = 2
DB size = 76K

RAM size = 4M

SIMM: Installed
WAN2: Not Installed
Compression: Not Installed
V.32 Modem: Installed
Encryption: Not Installed

Press any key to continue:

Figure G-8. System Information

10BaseT interface 2-4, C-1

A

Action, configure for bridge static address 5-49

Address

aging time, bridge; configure 5-47

default route, IP 5-40

Ethernet (MAC), LAN interface 5-8

IP, configure 5-16

IPX internal network number, configure 5-45

IPX network number, configure 5-24

static (bridging) 5-48

static address, bridge; configure 5-48, 5-49

static route, IP; configure 5-42

trap client 9-2

Address resolution protocol B-16

Aging

address (bridging) 5-47

IPX RIP age timer, configure 5-26

SAP age timer, configure 5-26

Annex D status (Frame Relay) 4-13, 4-15-17

ARP B-16

ARP table 4-39

Authentication traps, SNMP 9-2

Auto answer, dial-in management 7-2

Autolearn clients, SNMP 9-2

B

Bandwidth, WAN utilization 4-14

BCP status 4-27

BootP, download software G-1

Bridging

bridging table 4-52

enable, disable 5-13

global options, configure 5-46

status 4-45, 4-46

Broadcast (bridging) 5-46

C

Cables, part numbers C-2

Client address, SNMP 9-2

Community strings, SNMP 9-2

Configuration

start up 2-7

Configuration and software update 6-1

Connectors 2-4

Console

interface 2-4

password 8-2

Counters, error (CSU) 4-9

CSU

configuration screen 5-6

status and test 4-8

Customer support 10-1

D

DDD interface C-1

Default route

announce; enable, disable 5-21

global options, configure 5-40

Defaults restart 8-3

Diagnostic mode G-1

Diagnostic packets, IPX 5-27

Diagnostics, start-up 3-3, G-1

Dial-in access 1-2

Dial-in management 2-6

DLCI status 4-16

DLCI, frame relay 5-13

Dotted decimal notation B-6

E

Encryption

frame relay; enable, disable 5-14

global options, configure 5-51

Encryption options 5-37

Equipment return and repair 10-1

Error counters, CSU 4-9

Error threshold (configure for frame relay) 5-10

Ethernet B-2

F

File transfer 6-1

Filter mask, IPX SAP; configure 5-29

Filter State, IPX SAP; enable, disable 5-29

Filters, bridging

enable, disable 5-34

Transmit filter, configure 5-35

transmit filters 5-35

Filters, IP B-22

enable, disable for port 5-21

RIP Output Filter Table, configure 5-23

RIP, configure 5-22

Filters, IPX

RIP input/output filters 5-32

RIP/SAP input/output; enable, disable 5-27

SAP input, output filters; configure 5-29

Firmware version 8-6

Flash 2-9

Flash boot G-1
Frame Flooding, bridge; enable, disable 5-34
Frame relay 5-10, B-4
 encryption; enable, disable 5-14
 protocol options, configure 5-10
 protocol, configure 5-10
 status, Annex D 4-13, 4-15-17
 WAN status 4-13
Frame Type
 ethernet, configure 5-18
 IPX, configure 5-24
Full Enquiry Interval (configure for frame relay) .. 5-10

G

Gap time, IPX RIP/SAP; configure 5-45
Global configuration 5-39
Glossary A-1

H

Header, terminal screens 8-2
Hop Count
 too large, ICMP 4-33
 too large, IP 4-33
 too large, IPX 4-41
 too large, Netbios 4-42
Hop count (metric) 5-18
Hops, IPX 4-50
Host number B-6

I

ICMP status 4-33
Inactivity timeout, terminal 8-2
Input datagrams 4-30
Installation checklist 2-1
Interface
 configuration summary 5-7
 map to port 5-13
 status summary screen 4-10
Interfaces C-1
 LAN 2-4
 modem 2-4
 terminal 2-4
 WAN 1 2-4
Internal Network Number, IPX; configure 5-45
Inverse ARP
 IP; enable, disable (WAN) 5-20
 IPX; enable, disable 5-26
IP address 5-16, B-6
IP filters 5-21, B-22
IP routes
 default B-20

 direct and learned B-20
 static B-20
IP routing B-6
 ARP table 4-39
 enable, disable 5-13
 global options, configure 5-40
 LAN 5-16
 routing table 4-47
 status 4-30
 WAN 5-19
IPCP status 4-25
IPX B-23
IPX routing
 enable, disable 5-13
 global options, configure 5-45
 options, configure 5-24
 RIP/SAP status 4-43
 routing table 4-49
 status 4-40
IPX services table 4-51
IPXCP status 4-26
IPXWAN
 enable, disable 5-24
 status 4-44

K

Key password 8-2
Key Update Time, encryption; configure 5-51
Keys; conventions & prompts 3-2

L

LAN
 configuration screen 5-8
 status screen 4-11
LAN interface 2-4, C-1
LCP status 4-22
LEDs 1-2, 2-3
Line requirements 2-2
Line status 4-9
Local area network B-2
Logoff 3-5
Loopback tests, CSU 4-8
Lower layer status 4-14

M

MAC address
 ARP 4-39
 configure for bridging static address 5-49
 LAN interface 5-8
Main menu 3-5
Maintenance services 10-1

- Management methods 1-2
 - Management screen 9-2
 - Maximum Number of Configuration Requests, PPP;
 - configure 5-50
 - Maximum Number of Termination Requests, PPP;
 - configure 5-50
 - Maximum Transmission Unit (MTU); configure for IP
 - (WAN) 5-20
 - Metric
 - configure, default route 5-40
 - configure, IP 5-18
 - static route, IP; configure 5-42
 - MIB, enterprise 2-9
 - Modem
 - connection 2-6
 - interface 2-4
 - Modem security 7-2
 - Modem, security password 7-2
 - Monitor events, configure (Frame Relay) 5-10
 - Multicast, transmit (bridge); enable, disable 5-34
 - Multipurpose label F-1, F-2
- N**
- Network address to filter, IPX SAP 5-29
 - Network number B-6
 - Network number, IPX; configure 5-24
 - Next hop
 - static route, IP; configure 5-42
 - Node address to filter, IPX SAP; configure 5-30
 - Novell watchdog spoofing 5-28
 - Numbered 5-24
- O**
- Offset, bridge transmit filter; configure 5-35
 - Ordering information D-1
 - Output datagrams 4-31
- P**
- Part numbers, cables C-2
 - Password
 - console 2-5, 3-4
 - key (encryption) 8-2
 - remote dial-in management 2-6
 - terminal and telnet 8-2
 - Periodic RIP Timer, IPX; configure 5-24
 - Periodic SAP Timer, IPX; configure 5-26
 - Physical (MAC) address, for ARP 4-39
 - Ping 4-28
 - Point-to-Point protocol B-3
 - Polling interval, configure (Frame Relay) 5-11
 - Polling Verification Timer Interval, configure (Frame
 - Relay) 5-11
 - Port
 - configuration 5-13
 - configuration summary 5-12
 - enable, disable 5-13
 - name, configure 5-13
 - negotiable options, LCP 4-24
 - static address, bridge; configure 5-49
 - status summary 4-18
 - status, frame relay 4-20
 - status, LAN 4-19
 - status, PPP 4-21
 - Port counters, IP 4-32
 - PPP B-3
 - global options, configure 5-50
 - status, BCP 4-27
 - status, IPCP 4-25
 - status, IPXCP 4-26
 - status, LCP 4-22
 - protocol
 - frame relay 5-10
 - LAN interface 5-8
 - PPP 5-10
 - WAN interface 5-9, 5-10
- Q**
- Quick start procedure 2-7
- R**
- R/O community string 9-2
 - R/W community string 9-2
 - Remote dial-in access 2-6
 - Respond to RDL 5-6
 - Restart software, defaults 8-3
 - Restart Timer, PPP; configure 5-50
 - Restart, system 8-3
 - Return goods authorization 10-1
 - RIP B-18
 - age timer 5-26
 - input filter, configure 5-22
 - input, output filters 5-32
 - neighbor list 5-40
 - RIP, IP
 - enable, disable 5-17
 - input/output filters 5-23
 - listen only; enable, disable 5-22
 - output filter, configure 5-22
 - RIP, IPX B-26
 - input/output filters 5-32
 - periodic update timer; configure 5-24

RIP, IPX status 4-43
Router summary 4-6

S

SAP B-28
 age timer 5-26
 filters B-29
 input, output filters 5-29
 input/output filters 5-29
 status 4-43

Save to flash 3-5

Screen structure

 configuration 5-2
 main menu 3-1
 management 9-1
 status and test 4-2
 TFTP 6-1
 unit 7-1, 8-1

Screens

 Annex D status 4-13, 4-15-17
 ARP Table 4-39
 BCP Status 4-27
 Bridging Global Configuration 5-46
 Bridging Status 4-45
 Bridging Table 4-52
 CSU Status and Test 4-8
 DLCI Status Table 4-16
 Encryption Global Configuration 5-51
 Encryption Options 5-37
 Event Log 4-53
 Global Configuration 5-39
 ICMP Status 4-33
 Interface Configuration Summary 5-7
 Interface Status 4-10
 IP Global Configuration 5-40
 IP RIP Input Filter Table 5-23
 IP RIP Output Filter Table 5-23
 IP Routing Table 4-47
 IP Static Route 5-42
 IP Static Route Table 5-42
 IP Status 4-30
 IPCP status 4-25
 IPX Filters 5-27
 IPX Global Configuration 5-45
 IPX RIP/SAP Status 4-43
 IPX Routing Table 4-49
 IPX SAP Input Filter Table 5-29
 IPX Services Table 4-51
 IPX Status 4-40
 IPXWAN Status 4-44
 LAN Configuration 5-8

 LAN Status 4-11
 LCP Status 4-22
 Lower Layer Status 4-14
 Main Menu 3-5
 Management 9-2
 Ping/Trace Route 4-28
 Port Bridging Status 4-46
 Port Configuration 5-13
 Port Configuration Summary 5-12
 Port Counters 4-32
 Port IP Filters (LAN) 5-21
 Port IP Routing Options 5-16, 5-19
 Port IPX Input Filter 5-32
 Port IPX Output Filter 5-32
 Port IPX RIP Input Filter Table 5-32
 Port IPX RIP Output Filter Table 5-32
 Port IPX Routing Options 5-24
 Port IPX SAP Output Filter Table 5-29
 Port Status 4-18, 4-19
 PPP Global Configuration 5-50
 Service Information 8-7
 SNMP Status 4-37
 Static Address Table, bridging 5-48
 Static Address, bridging 5-48
 System Information 8-6
 System Restart 8-3
 TCP and UDP Status 4-34
 TCP Connection Table 4-36
 TCP/IP Status 4-28
 Transmit Filter 5-35
 Transmit Filter Table 5-35
 Unit 8-2
 WAN 1 Configuration 5-9
 WAN 1 Protocol Options (Frame Relay) 5-10
 WAN Status (Frame Relay) 4-13
 Security password, dial-in management 7-2
 Security password, modem 7-2
 Serialization packets, IPX 5-27
 Server name to filter, IPX SAP; configure 5-30
 Server type to filter, IPX SAP; configure 5-30
 Service Advertising Protocol (SAP) B-28
 Service information 8-7
 Service, phone number 10-1
 SNMP 1-2, 2-5
 client address 9-2
 options 9-1
 read only community string 9-2
 read/write community string 9-2
 status 4-37
 Software update 6-1
 Software version 8-6
 Source quench 4-33

-
- Specifications E-1
 - Start-up diagnostics 3-3, G-1
 - Start-up procedure, initial 2-7
 - Static address (route)
 - bridging, configure 5-48, 5-49
 - IP, announce routes 5-21
 - IP, configure 5-42
 - Static route table 5-40
 - Subnet mask B-7
 - configure for port 5-16
 - IP routing table 4-47
 - request from a device 4-34
 - static route, IP; configure 5-42
 - Subnet zero 5-41
 - Subnetworking 5-42, B-7
 - subnet mask 5-16
 - Support plans 10-1
 - System information screen 8-6
 - System restart 8-3
 - System time 8-2
- T**
- TCP connection table 4-36
 - TCP status 4-34
 - TCP/IP status 4-28
 - Telephone numbers 8-7, 10-1
 - Telnet 1-2
 - enable, disable 9-2
 - Terminal
 - configuration 3-3
 - connect 2-8
 - management 2-5
 - selection 3-3
 - Tests
 - diagnostics G-1
 - diagnostics, start-up G-1
 - Tests; loopback, CSU 4-8
 - TFTP (Trivial File Transfer Protocol) 6-1
 - TFTP software download G-4
 - Time, system 8-2
 - Timing, network 5-6
 - Trace route 4-28
 - Traceroute 4-28
 - Transmit broadcast, bridging 5-34
 - Transmit filter, bridge; configure 5-34
 - Transmit filter; bridging, configure 5-35
 - Transmit multicast, bridge; configure 5-34
 - Traps, SNMP 9-2, 9-3
 - Type 20 hop count 4-42
 - Type 20 packets, IPX 5-28
 - Type Value, bridge transmit filter; configure 5-35
- U**
- UDP status 4-34
 - Unit screen 8-2
 - Unnumbered 5-24
 - Upload/download files (TFTP) 6-4
 - Utilization, WAN 4-14
- V**
- V.32 modem 1-2
 - dial-in management 2-6
 - V.32 modem interface C-1
- W**
- WAN
- protocol options, configure (frame relay) 5-10
 - WAN 1 interface 2-4, C-1
 - WAN 2 interface 2-4
 - WAN status screen 4-13, 4-17
 - WAN to WAN forwarding (bridge) 5-47
 - WAN utilization 4-14
 - Watchdog packets 5-28
 - Watchdog spoofing B-24
-

